

CQR-981

Wireless-N Pico 3.5G Broadband Router



User Manual

Version 1.00
(Sep, 2010)

Table of Contents

TABLE OF CONTENTS.....	2
PREFACE	5
CHAPTER 1 INTRODUCTION.....	6
1.1 About CQR-981	6
1.2 Main Features	6
1.3 System Requirements.....	6
1.4 Getting to Know CQR-981	7
1.4.1 Hardware Specifications.....	8
CHAPTER 2 SYSTEM AND NETWORK SETUP.....	9
2.1 Build Network Connection (Router mode)	9
2.2 Build Network Connection (AP mode)	10
2.3 Build Network Connection (WiFi-AP mode)	11
2.4 Connecting to CQR-981 by using Web Browser	12
2.4.1 Windows 95/98/ME	12
2.4.2 Windows 2000	14
2.4.3 Windows XP	16
2.4.4 Windows Vista / Windows 7.....	18
2.4.5 Router IP Address Lookup	20
2.4.6 Connect the Wireless Router's management Interface by Web Browser	21
CHAPTER 3 ONE BUTTON SETUP CONFIGURATION	23
CHAPTER 4 ROUTER MODE ADVANCED CONFIGURATION.....	25
4.1 IP Configuration.....	25
4.1.1 WAN Interface Setup.....	25
4.1.1.1 WAN Interface – Ethernet Port	26
4.1.1.1.1 WAN Access Type – Static IP	27
4.1.1.1.2 WAN Access -- Dynamic IP	30
4.1.1.1.3 WAN Access Type -- PPPoE.....	33
4.1.1.1.4 WAN Access Type -- PPTP.....	36
4.1.1.1.5 WAN Access Type – L2TP.....	39
4.1.1.2 WAN Interface – 3.5G (HSDPA/UMTS)	42
4.1.1.3 WAN Access Type – WiMAX.....	45
4.1.1.4 WAN Access Type – Wireless	47
4.1.2 LAN Interface Setup	48
4.1.3 Dynamic DNS Setting.....	49
4.2 Wireless Setup	51
4.2.1 Wireless Basic Settings.....	51
4.2.1.1 Multiple APs	54
4.2.1.2 Enable Universal Repeater Mode (Acting as AP Client simultaneously).....	55
4.2.2 Wireless Advanced Settings	57
4.2.3 Wireless Security Setup	59

4.2.4	Wireless Access Control	61
4.2.5	WDS Settings	64
4.2.6	WPS	70
4.3	NAT	77
4.3.1	Virtual Server	77
4.3.2	DMZ.....	78
4.4	Firewall.....	79
4.4.1	Port Filtering	80
4.4.2	IP Filtering	81
4.4.3	MAC Filtering	82
4.4.4	URL Filtering.....	83
4.5	System Management	84
4.5.1	Change Password	84
4.5.2	Firmware Upgrade	85
4.5.3	Profile Save.....	86
4.5.4	Time Zone Setting	90
4.5.5	UPnP Setting.....	91
4.6	Log & Status	92
4.6.1	Network Config	92
4.6.2	Event Log	93
4.7	Logout	94
CHAPTER 5	AP MODE ADVANCED CONFIGURATION	95
5.1	IP Config	95
5.1.1	LAN Setup.....	95
5.1.2	LAN Interface Setup	95
5.2	Wireless Setup	97
5.2.1	Wireless Basic Settings.....	97
5.2.1.1	Multiple APs	99
5.2.2	Wireless Advanced Settings	100
5.2.3	Wireless Security Setup	102
5.2.4	Wireless Access Control	104
5.2.5	WDS Settings	106
5.2.6	WPS	112
5.3	System Management	119
5.3.1	Change Password	119
5.3.2	Firmware Upgrade	119
5.3.1	Profile Save.....	121
5.3.2	Time Zone Setting	126
5.3.3	UPnP Setting.....	127
5.3.4	Log & Status	128
5.3.5	Network Config	128
5.3.6	Event Log	128
5.4	Logout	130
CHAPTER 6	ADVANCED CONFIGURATION FOR WI-FI AP MODE	131
6.1	IP Config	131

6.1.1	IP Config -- LAN	131
6.1.2	LAN Interface Setup	131
6.2	Wireless Setup	133
6.2.1	Wireless Basic Setting	133
6.2.2	Wireless Advanced Settings	136
6.2.3	Wireless Site Survey	138
6.2.4	Wireless Security Setup	138
6.2.5	Wireless Access Control	141
6.2.6	WPS Setting	143
6.3	System Management	149
6.3.1	Change Password	149
6.3.2	Firmware Upgrade	150
6.3.1	Profile Save	151
6.3.2	Time Zone Setting	155
6.3.3	UPnP Setting	156
6.4	Log & Status	156
6.4.1	Network Config	157
6.4.2	Event Log	157
6.5	Logout	158
CHAPTER 7	DDNS ACCOUNT SETUP	159
CHAPTER 8	Q & A	165
8.1	Installation	165
8.2	LED	165
8.3	IP Address	166
8.4	OS Setting	166
8.5	11n Broadband Router Setup	167
8.6	Wireless LAN	169
8.7	Support	171
8.8	Others	172

Preface

About This Manual

Thank you for purchasing the CQR-981 Wireless-N Pico 3.5G Broadband Router. This User's Manual is intended for audience with basic networking knowledge and is the primary reference for configuring and maintaining the device. This manual includes description of the management interface and detailed instruction in its use.

Conventions Used

- Notes, warnings or cautions are in bold with shaded background.
- In this manual, the CQR-981 Wireless-N Pico 3.5G Broadband Router is referred to as “the wireless router”.

Chapter 1 Introduction

1.1 About CQR-981

CQR-981 is a tiny name card size mini broadband router; it's easy to carry while providing wired Ethernet, Wireless, 3.5G and WiMAX interfaces to meet the requirement of different user groups. With CQR-981, users can share the internet connection and resources anywhere, anytime. Additionally its automatically detection of the user's environment settings brings convenience of plug and play and makes internet experience more enjoyable.

While sharing internet connection with other computers, security mechanisms such as WEP/WPA/WPS can be used to ensure the security level of networking environment.

CQR-981 is a networking solution product designed for mobile business and personal applications, it's not only secure, reliable but also easy to operate and use.

1.2 Main Features

The following lists are the main features of the Wireless Router

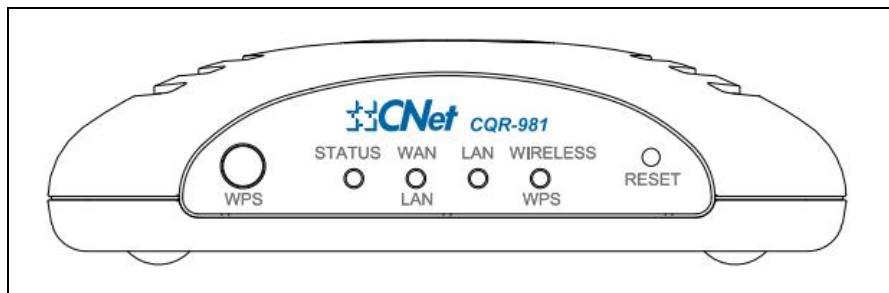
- Mini name card sized design for ease of carrying.
- Support mini USB power DC input.
- Auto detecting WAN type for easier setup.
- 1T1R wireless solution provides reasonable wireless performance.
- Supports WPS for easy wireless connection setup
- Supports Multiple-AP application (up to 4 SSIDs)
- Advanced wireless security, WEP/WPA/WPA2/WPA2 Mixed
- Complies with IEEE 802.11b/g and IEEE 802.11n

1.3 System Requirements

- Internet connections provided via xDSL/cable modem with a RJ-45 Ethernet port or 3.5G/WiMAX mobile Internet connections.
- Computer or network devices with wired or wireless network interface card.
- Web browser (*Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, or Safari web browser*).
- An available AC power socket.

1.4 Getting to Know CQR-981

The front view of CQR-981



LED	Function	Color	Status	Description
STATUS x 1	System status	Green	On	System is ready to work
			Blinking	1. Power is being applied and system boot in progress 2. Reset or firmware upgrade in progress
WAN / LAN x 1	WAN port activity	Green	On	100Mbps Ethernet is connected
			Blinking (Fast)	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking (Slow)	10Mbps Ethernet Tx/Rx activity
LAN x 1	LAN port activity	Green	On	100Mbps Ethernet is connected
			Blinking (Fast)	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking (Slow)	10Mbps Ethernet Tx/Rx activity
Wireless / WPS x 1	Wireless activity & WPS status	Green	On	Wireless is connected
			Blinking (Fast)	Wireless Tx/Rx activity
		Orange	Blinking (Slow)	WPS function in progress

1.4.1 Hardware Specifications

The following table shows the technical specifications of the wireless router.

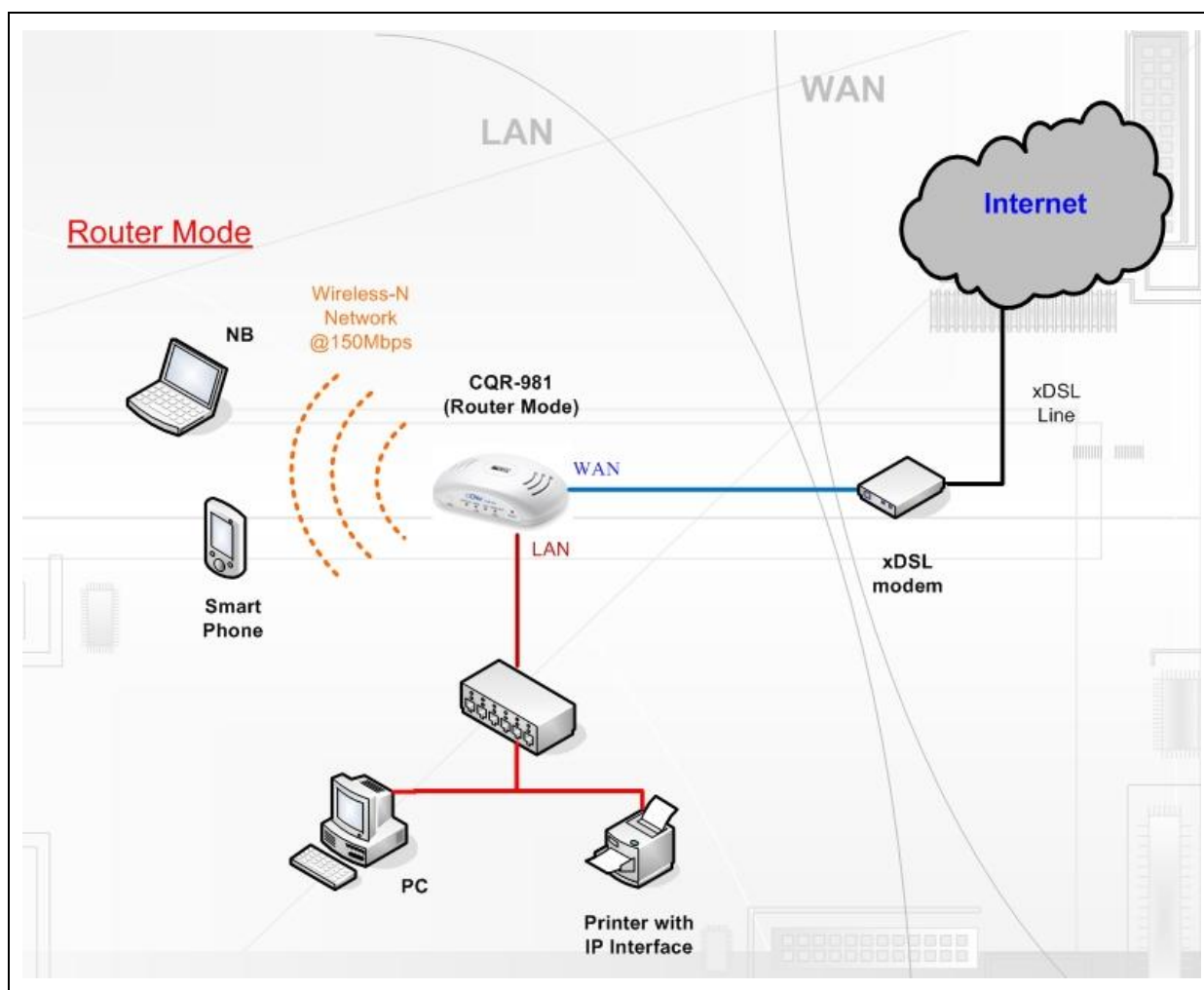
Item	Specifications
Communication Interface	
WAN/LAN Port	1 x 10/100Mbps RJ-45, with auto MDI/MDIX
LAN Port	1 x 10/100Mbps RJ-45, with auto MDI/MDIX
USB Port	USB 2.0 port x 1
Wireless	IEEE 802.11b/g/n
Others	
Operation Requirement	Operating Temp: 0° to 40°C (32° to 10°F) Storage Temp: -20° to 70°C (-4° to 158°F) Operating Humidity: 10% to 85% Non-Condensing Storage Humidity: 5% to 90% Non-Condensing
Sessions	20,000
Antenna	Internal x 1
Peak Gain of the antenna	2dBi@ 2.45GHz
Transmitted Power	IEEE 802.11b: 19dBm +/- 2.0dBm (typical) IEEE 802.11g: 16dBm +/- 2.0dBm (typical) IEEE 802.11n: 14dBm +/- 1.5dBm (typical)
Receive Sensitivity	IEEE 802.11b: -83dBm +/- 2.0dBm IEEE 802.11g: -70dBm +/- 2.0dBm IEEE 802.11n (20MHz): -74dBm +/- 2.0dBm IEEE 802.11n (20MHz): -74dBm +/- 2.0dBm
Dimension (L x W x H)	88(L) x 58(W) x 26.5(H) mm
Button	Reboot / Reset button WPS button
Power Supply	Power Adapter DC5V/1.0A with mini-USB B type male connector
Certification	CE / FCC / RoHS

Chapter 2 System and Network Setup

The CQR-981 is an easy to setup and wireless device for various application and environment. It can be used in conference room, hotel, even in transportation.

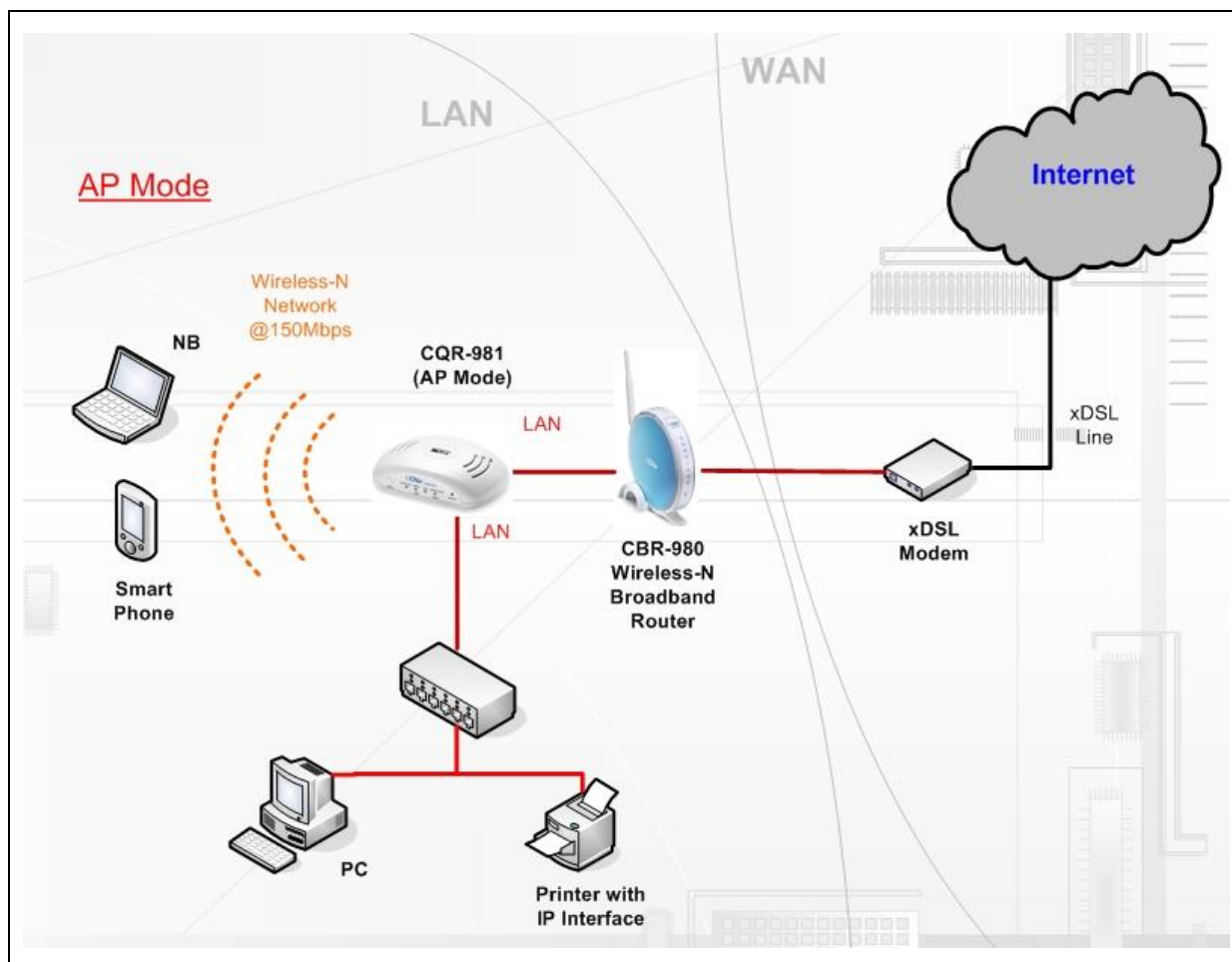
2.1 Build Network Connection (Router mode)

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.



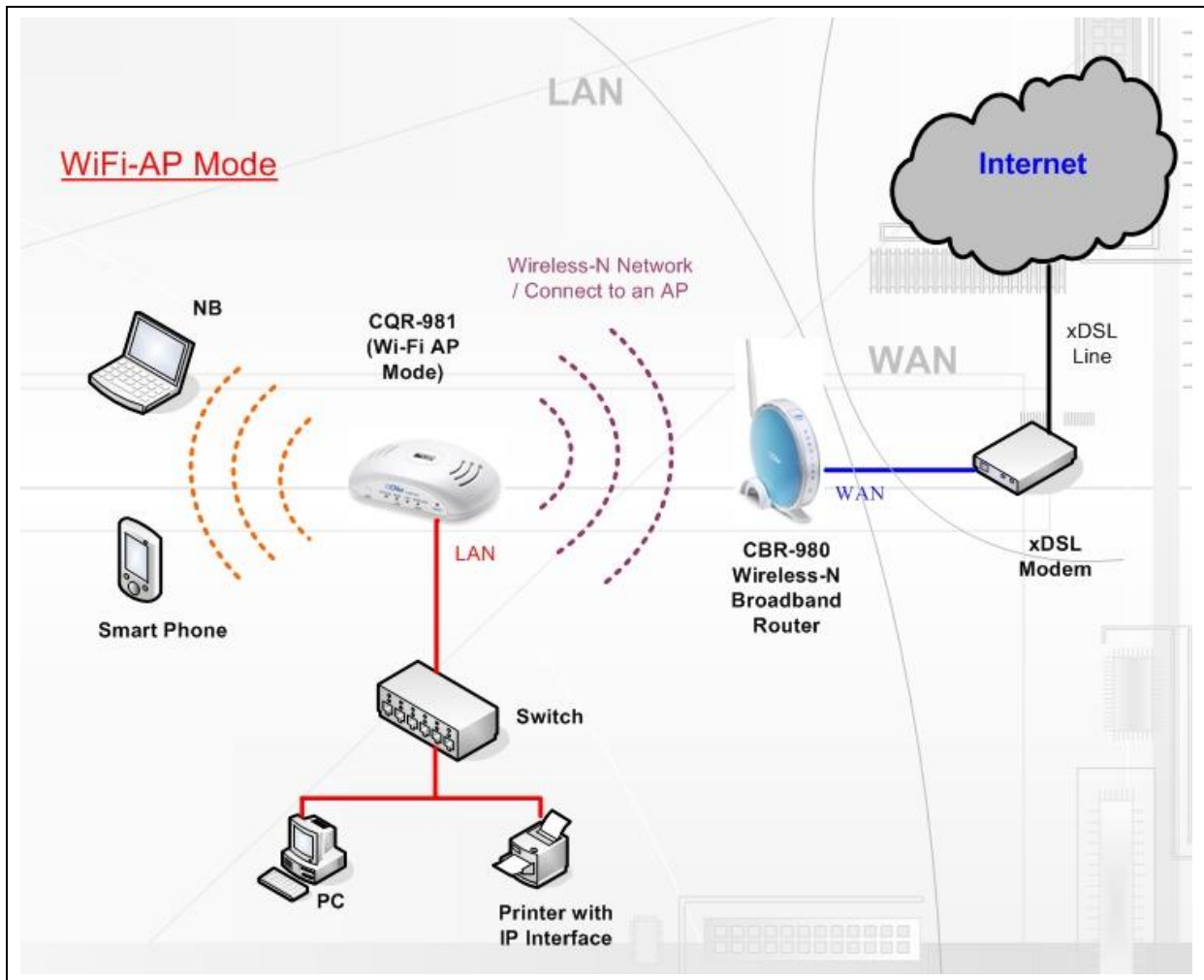
2.2 Build Network Connection (AP mode)

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.



2.3 Build Network Connection (WiFi-AP mode)

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.



2.4 Connecting to CQR-981 by using Web Browser

After the network connection is built, the next step what you should do is setup the router with proper network parameters, so it can work properly in your network environment.

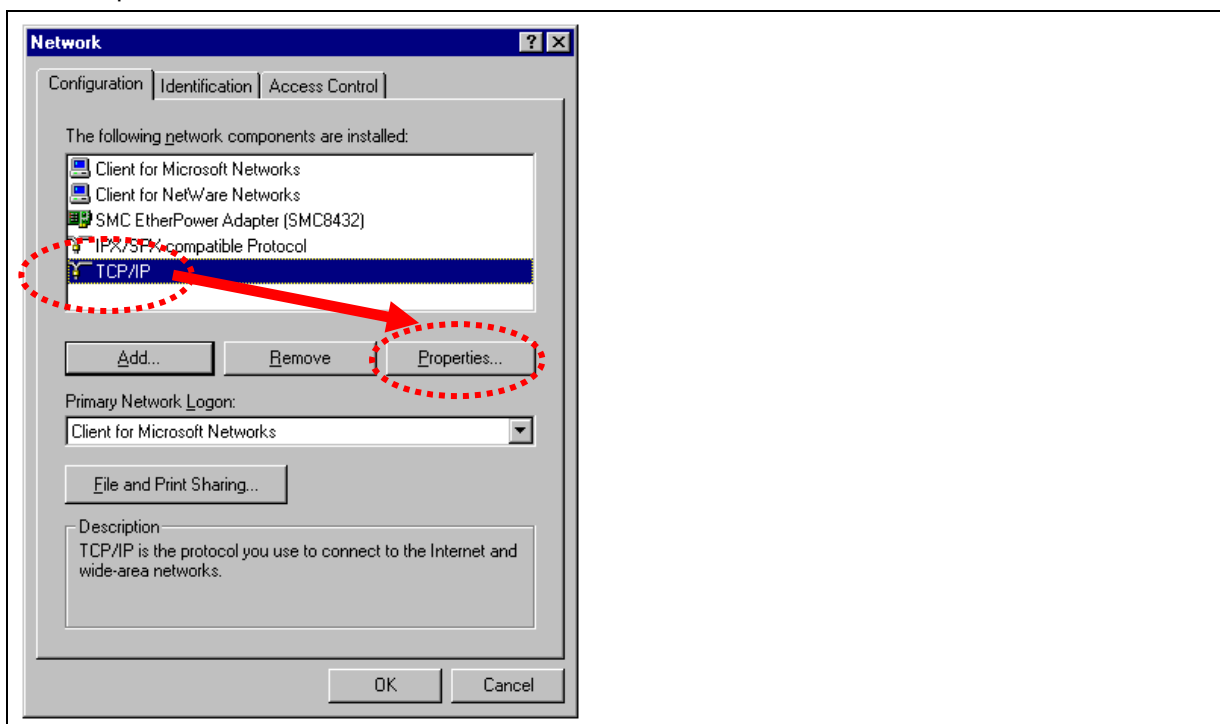
Before you connect to the wireless router and start configuration procedures, your computer must be able to get an IP address from the wireless router automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the below instructions to configure your computer with dynamic IP address:

If the operating system of your computer is....

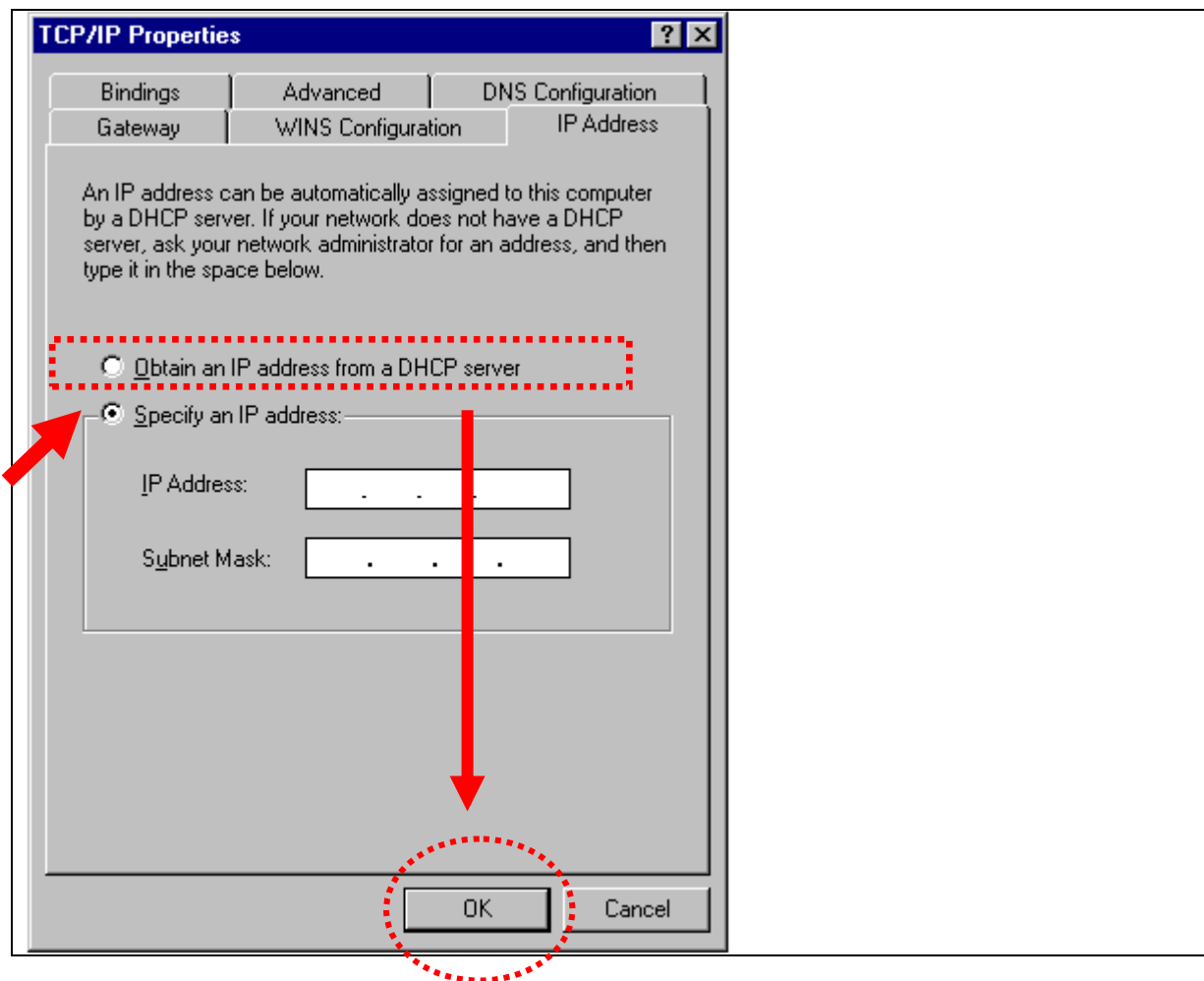
- Windows 95/98/ME** - please go to section 2.4.1
- Windows 2000** - please go to section 2.4.2
- Windows XP** - please go to section 2.4.3
- Windows Vista/7** - please go to section 2.4.4

2.4.1 Windows 95/98/ME

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network** icon, and **Network** window will appear. Select '**TCP/IP**', then click 'Properties'.

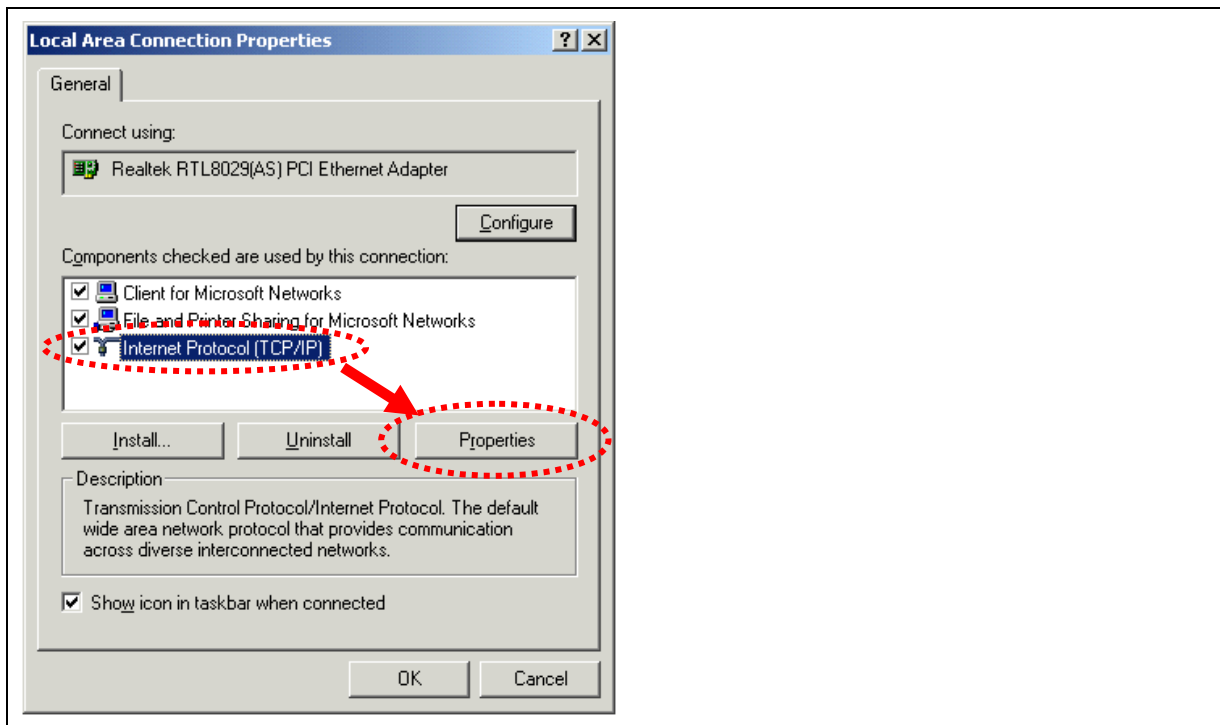


2. Select '**Obtain an IP address from a DHCP server**', and then click 'OK'.

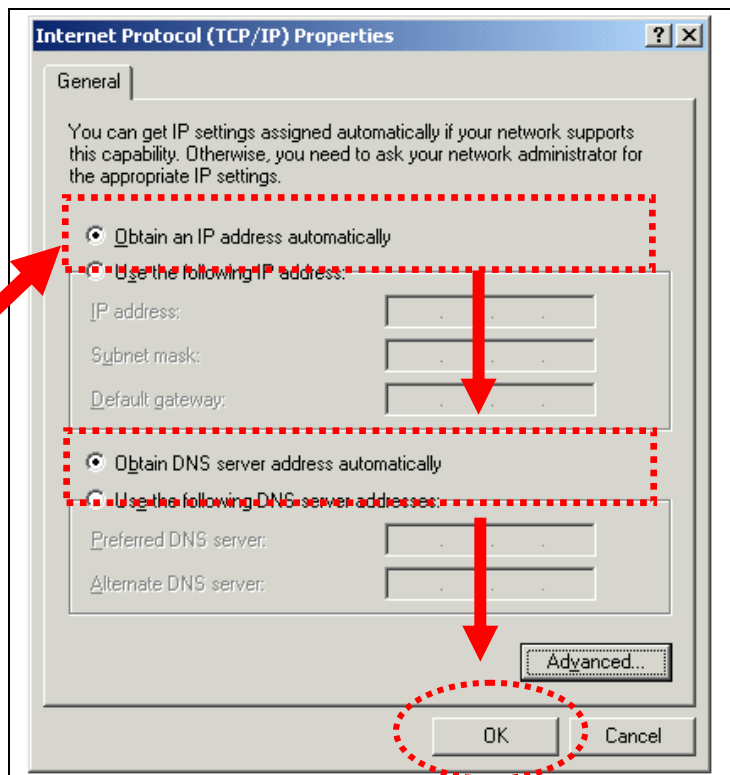


2.4.2 Windows 2000

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection**, and **Local Area Connection Properties** window will appear. Select '**Internet Protocol (TCP/IP)**', then click '**Properties**'.

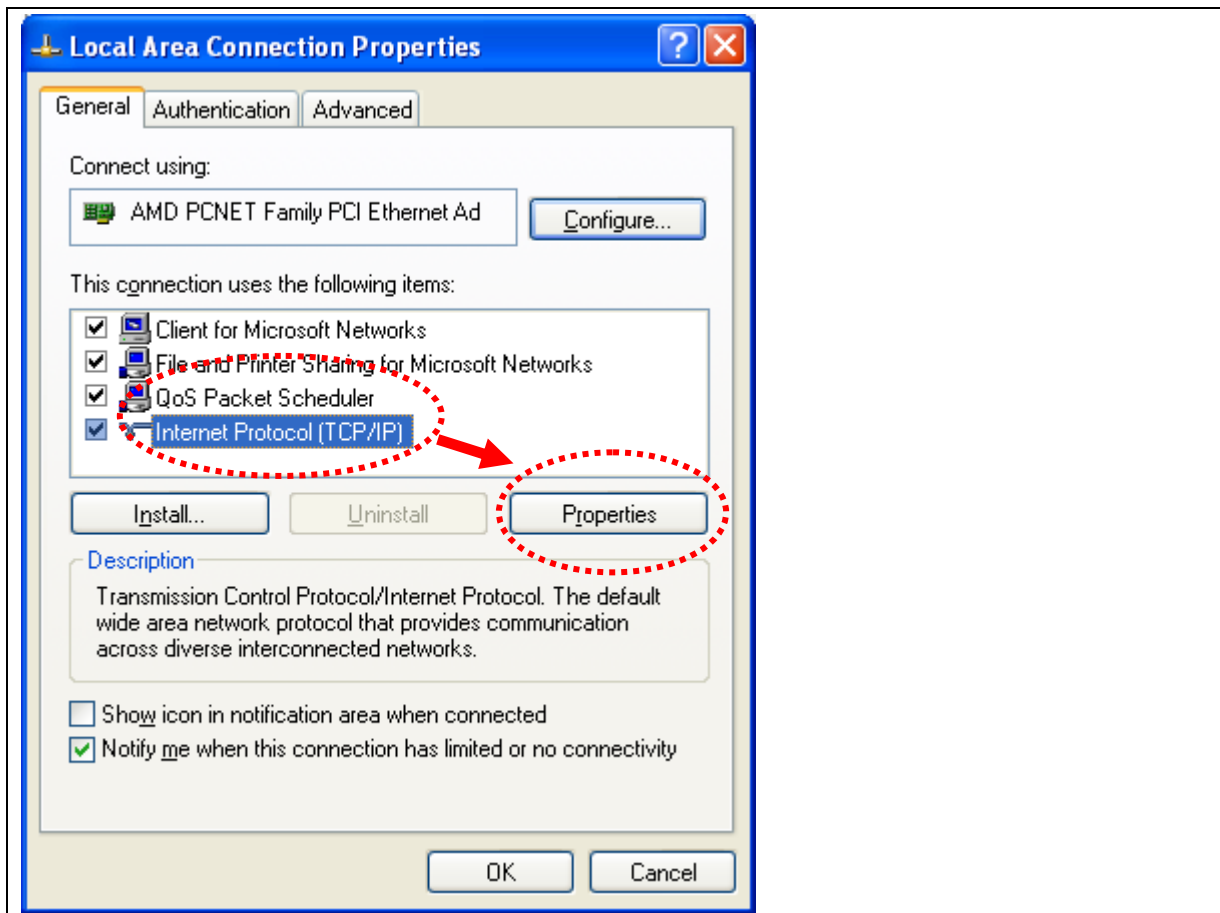


2. Select '**Obtain an IP address automatically**' and '**Obtain DNS server address automatically**', then click '**OK**'.

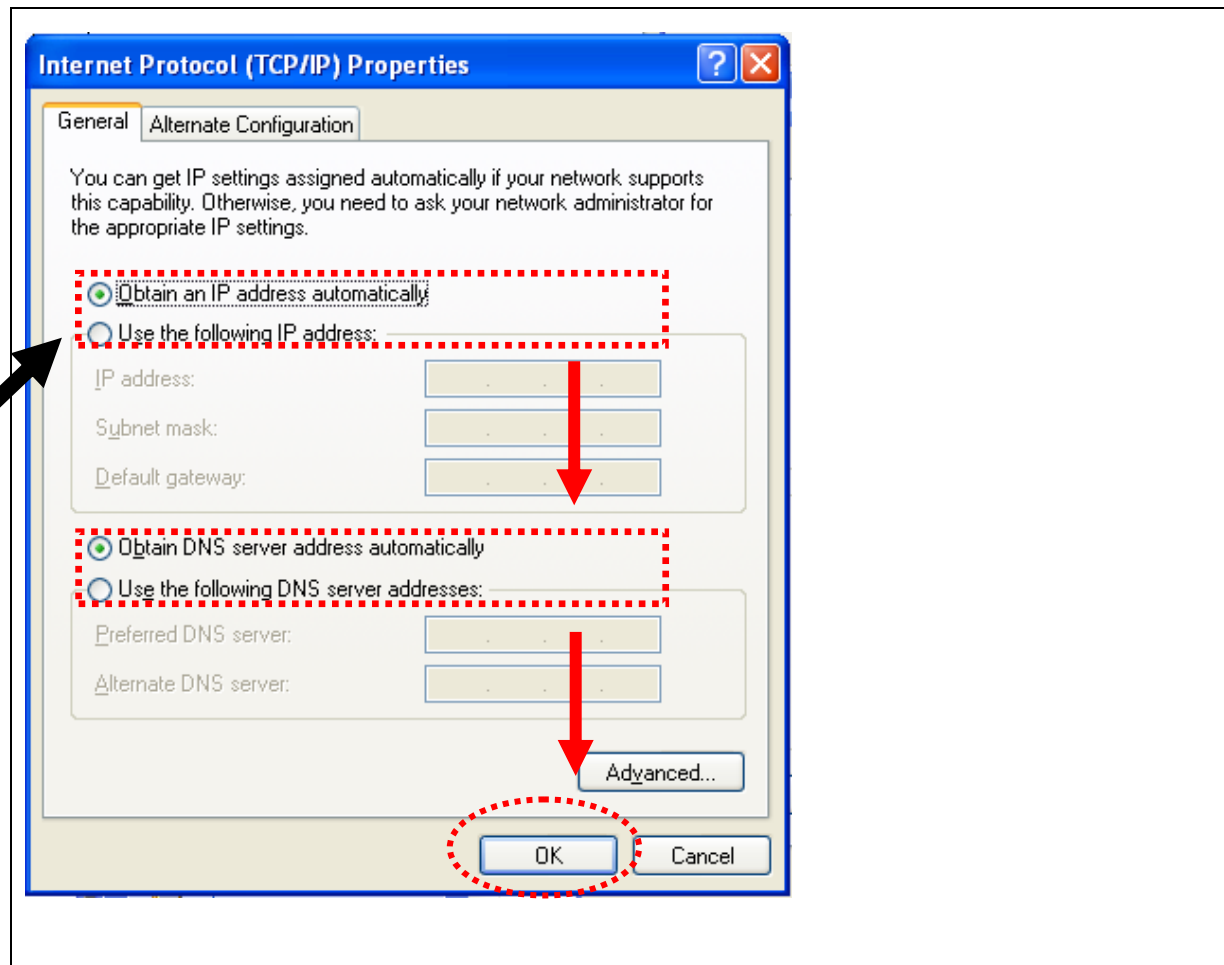


2.4.3 Windows XP

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections**, then double-click **Local Area Connection**, **Local Area Connection Status** window will appear, and then click '**Properties**'.

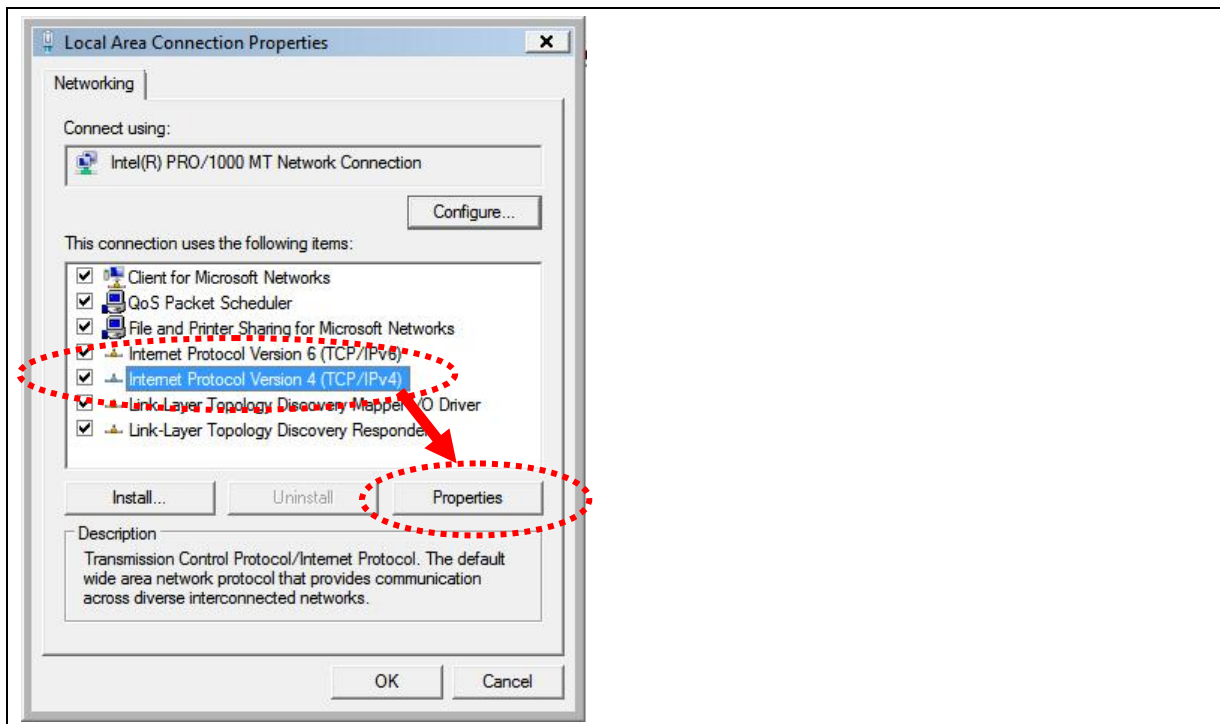


2. Select '**Obtain an IP address automatically**' and '**Obtain DNS server address automatically**', then click '**OK**'.

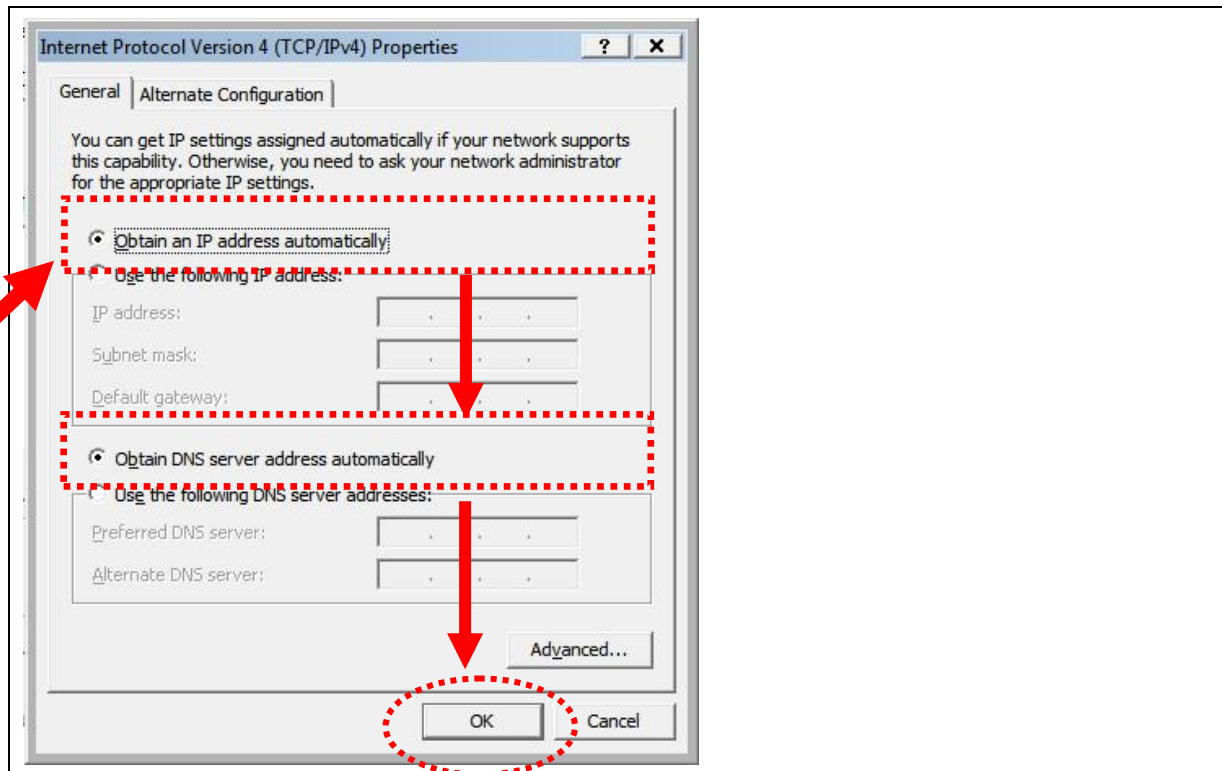


2.4.4 Windows Vista / Windows 7

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Click **View Network Status and Tasks**, and then click **Manage Network Connections**. Right-click **Local Area Network**, then select '**Properties**'. **Local Area Connection Properties** window will appear, select '**Internet Protocol Version 4 (TCP / IPv4)**', and then click '**Properties**'.

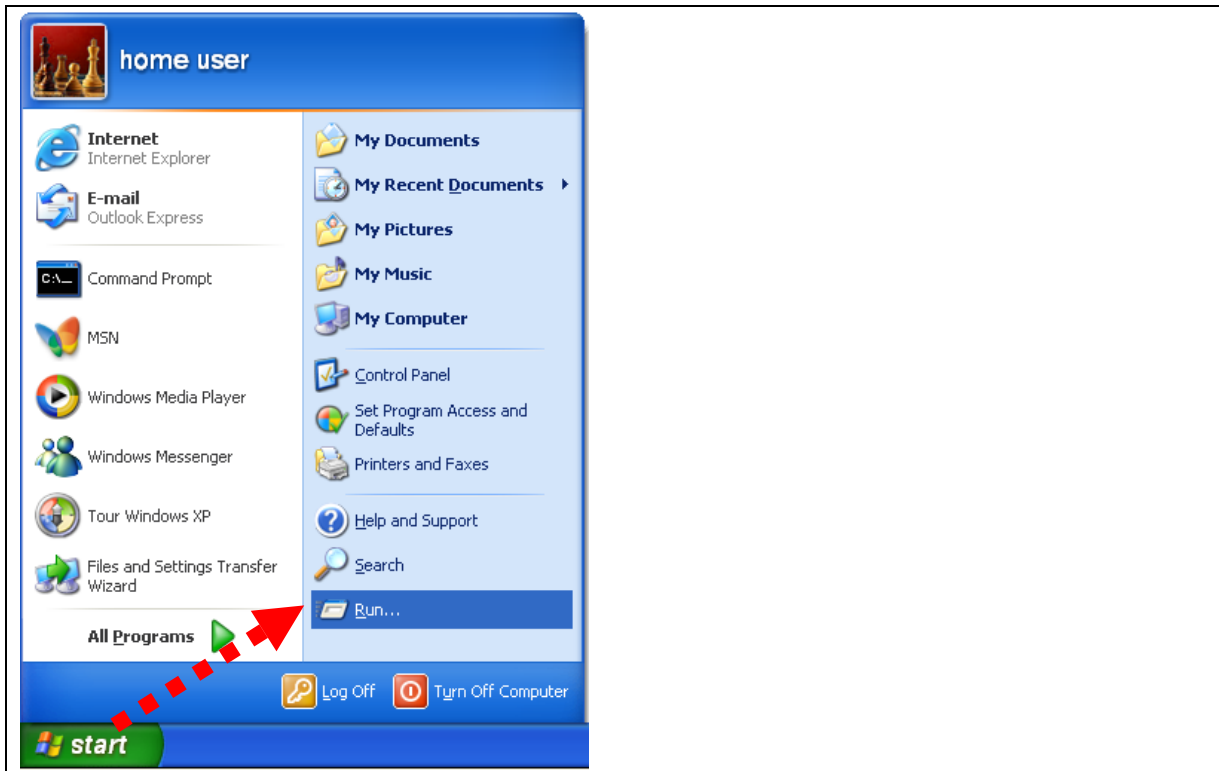


2. Select '**Obtain an IP address automatically**' and '**Obtain DNS server address automatically**', then click 'OK'.

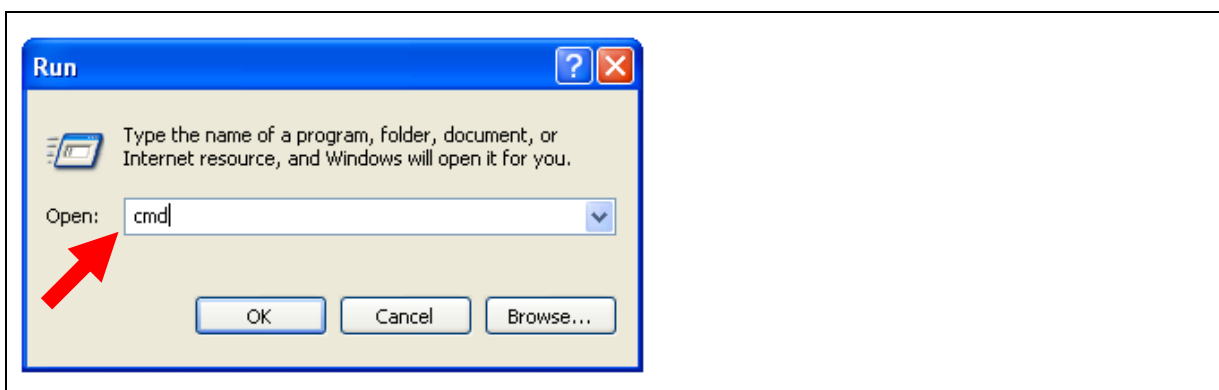


2.4.5 Router IP Address Lookup

After the IP address setup was completed, please clicks '**Start**' → '**run**' at the bottom-lower corner of your desktop:



Input '**cmd**', and then click '**OK**'



Input '**ipconfig**', then press '**Enter**' key. Please check the IP address followed by '**Default Gateway**' (In this example, the gateway IP address of router is 192.168.1.1)

```

C:\Documents and Settings\demo>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1
C:\Documents and Settings\demo>

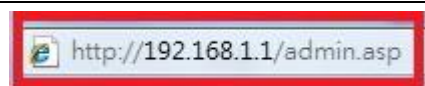
```

NOTE: If the IP address of Gateway is not displayed, or the address followed by 'IP Address' begins with '169.x.x.x', please recheck network connection between your computer and router, and / or go to the beginning of this chapter, to recheck every step of network setup procedure.

2.4.6 Connect the Wireless Router's management Interface by Web Browser

After your computer obtained an IP address from wireless router, please start your web browser, and input the IP address of the wireless router in address bar, and the following message should be shown. Please click "**Administrator**" to login the CQR-981.

Notes: The default IP of the wireless router is 192.168.1.1



Please input user name and password in the field respectively. Default user name is '**admin**', and default password is '**admin**', then press '**Login**' button to login the web management interface of the wireless router.

Router

- One Button Setup
- + IP Config
- + Wireless
- + NAT
- + Firewall
- + System Management
- + Log and Status
- Logout

Network Config

This page shows the current status and some basic settings of the device.

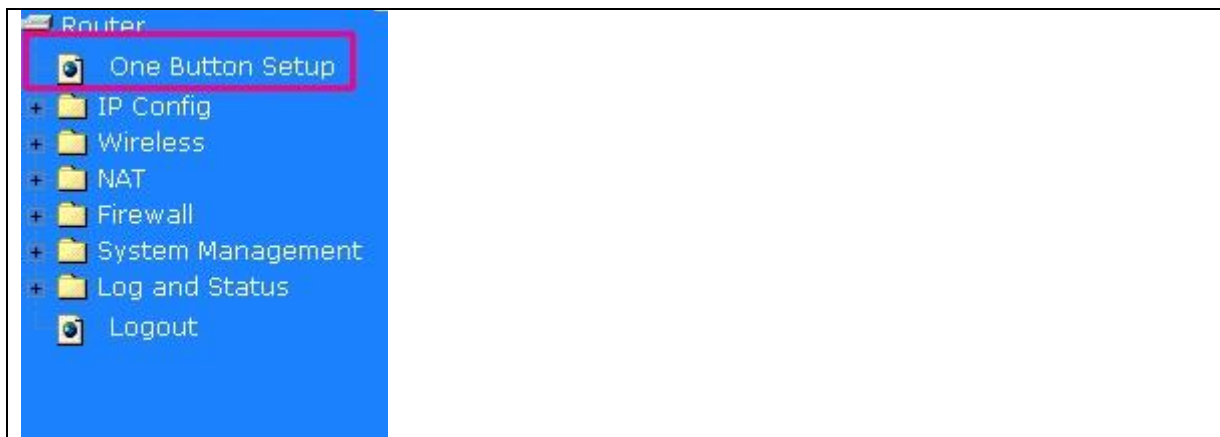
System	
Uptime	0day:1h:46m:51s
Firmware Version	Ver1.0.2
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CQR-981
Channel Number	6
Encryption	Disabled
MAC Address	00:08:a1:c7:a5:2b
Associated Clients	1
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:08:a1:c7:a5:2b
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:08:a1:c7:a5:2c
3.5G Configuration	

NOTE: If you can't see the web management interface, and you're being prompted to input user name and password again, it means you didn't input username and password correctly. Please retype user name and password again. If you're certain about the user name and password what you type are correct, please go to 'Troubleshooting' to perform a factory reset, to set the password back to the default value.

Chapter 3 One Button Setup Configuration

CQR-981's **"One Button Setup"** will help you to setup the basic setting of the wireless router with simplified procedure. You do not need to learn much complicated network proper name but you still can setup the wireless router by yourself.

Please click **"One Button Setup"** function, and then click the "finish" to complete the setting. The router will reboot automatically.



One Button Setup

This page is used to configure all of the server router function for first time.

Time Zone Select
Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana


Change Password
New Password:

WAN Interface Setup
WAN Interface: Ethernet Port

WAN Type Setup
WAN Access Type: Dynamic IP

Wireless Setup
SSID:
Encryption: None

Finish

Item	Description
Time Zone Select	Press  button to choose a time zone of the location you live from the drop-down list.
Change Password	Input new password here
Device Name	Input new device name here
WAN Interface Setup	<p>Choose the broadband interface you are using. The wireless router supports Ethernet Port / Wireless / 3.5G / WiMAX 4 different types of interface.</p> <p>Please refer to Chapter 4.1.1 for details about all WAN type settings.</p>
Wireless Setup	Configure Wireless SSID and Security.
Finish	Click finish button to complete the setting

Chapter 4 Router Mode Advanced Configuration

This chapter describes how to setup the access the router through the web browser. Please be noted that in order to access the router's admin page, a computer must be connected to one of the LAN ports on the router. The WLAN Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: 192.168.1.1

Default IP subnet mask: 255.255.255.0

WEB login User Name: admin

WEB login Password: admin

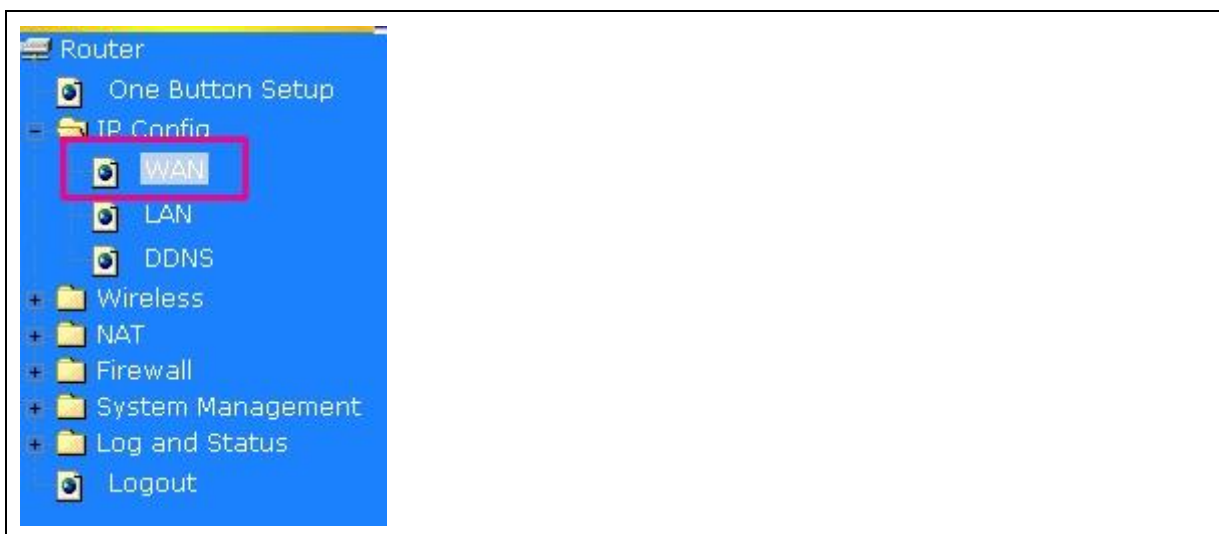
4.1 IP Configuration

In this section that user could configure the connection type of WAN port. Please check with your Internet Service Provider about the essential connection parameter.

4.1.1 WAN Interface Setup

Select **WAN** under the **IP Config** menu. CQR-981 supports 4 interfaces and 5 access types. Follow the instructions below for each to set up accordingly.

Choose your WAN Interface and WAN type, and click **Next**, its associated settings will show up.



4.1.1.1 WAN Interface – Ethernet Port

If you are using an Ethernet cable to connect the Internet, please select **Ethernet port**.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface:	<input type="text" value="Ethernet Port"/>
WAN Access Type:	<input type="text" value="DHCP Client"/>
Host Name:	<input type="text" value="default"/>
MTU Size:	<input type="text" value="1492"/> (1400-1492 bytes)
<input checked="" type="radio"/> Attain DNS Automatically	
<input type="radio"/> Set DNS Manually	
DNS 1:	<input type="text"/>
DNS 2:	<input type="text"/>
DNS 3:	<input type="text"/>
3.5G Backup:	<input checked="" type="checkbox"/> Backup of connection, check connection in every <input type="text" value="3"/> minutes.
Service:	<input type="text" value="UMTS/HSPA/HSDPA/HSUPA"/>
Connect Speed:	<input checked="" type="radio"/> Auto Switch <input type="radio"/> 2.5G/2.75G only <input type="radio"/> 3G/3.5G only
SIM PIN:	<input type="text"/> <input checked="" type="checkbox"/> None
Retype SIM PIN:	<input type="text"/>
APN:	<input type="text" value="internet"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
PHONE Number:	<input type="text" value="*99#"/>
Clone MAC Address:	<input type="text" value="000000000000"/>
<input checked="" type="checkbox"/> Enable IGMP Proxy	
<input checked="" type="checkbox"/> Enable Ping Access on WAN	
<input checked="" type="checkbox"/> Enable Web Server Access on WAN	
<input type="button" value="Apply Change"/> <input type="button" value="Reset"/>	

4.1.1.1.1 WAN Access Type – Static IP

If you applied for a **Static IP** connection type from ISP, please follow the steps to set up your WAN connection.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface:

Ethernet Port

WAN Access Type:

Static IP

IP Address:

172.1.1.1

Subnet Mask:

255.255.255.0

Default Gateway:

172.1.1.254

MTU Size:

1500

(1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

3.5G Backup:

☒ Backup of connection, check connection in every 3 minutes.

Service:

UMTS/HSPA/HSDPA/HSUPA

Connect Speed:

☒ Auto Switch ☐ 2.5G/2.75G only ☐ 3G/3.5G only

SIM PIN:

☒ None

Retype SIM PIN:

APN:

internet

User Name:

Password:

PHONE Number:

*99#

Clone MAC Address:

000000000000

☒ Enable IGMP Proxy

☒ Enable Ping Access on WAN

☒ Enable Web Server Access on WAN

Apply Change

Reset

Item	Description
IP Address	Please enter the IP address which is provided by your ISP. If you don't have it, please contact your ISP.
Subnet Mask	Please enter the Subnet Mask address.

Default Gateway	Input ISP Default Gateway Address. If you don't know, please check with your ISP.
MTU Size	The term Maximum transmission unit refers to the size (in bytes) of the largest PDU that a given layer of a communications protocol can pass onwards. Users can improve network efficiency by adjusting the value of MTU. Most of OS will give users a default value which is fit for most of users. Users can modify this value also. Please enter value, max number is 1500 bytes.
DNS	If ISP provides DNS information, please select Attain DNS automatically . Or you should select Set DNS Manually , and then input the DNS address.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP, default setting is internet .
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is *99# .
Clone MAC	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	To enable WAN ICMP response.

Enable Web Server Access on WAN	Enable Web Server Access function from WAN side.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.1.2 WAN Access -- Dynamic IP

If your WAN access type is **Dynamic IP**, please complete the settings as following instructions.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface:

Ethernet Port

WAN Access Type:

DHCP Client

Host Name:

default

MTU Size:

1492

(1400-1492 bytes)

☒ Attain DNS Automatically

☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

3.5G Backup:

☒ Backup of connection, check connection in every 3 minutes.

Service:

UMTS/HSPA/HSDPA/HSUPA

Connect Speed:

☒ Auto Switch ☐ 2.5G/2.75G only ☐ 3G/3.5G only

SIM PIN:

☒ None

Retype SIM PIN:

APN:

internet

User Name:

Password:

PHONE Number:

*99#

Clone MAC Address:

000000000000

☒ Enable IGMP Proxy

☒ Enable Ping Access on WAN

☒ Enable Web Server Access on WAN

Apply Change

Reset

Item	Description
Host Name	The host name is optional; but if your ISP requires you to input a specific host name, please put it in, for example, 11n Broadband Router applied from ISP. Generally, Cable Modem

	will provide the hostname information.
MTU Size	MTU stands for Maximum Transmission Unit. For Static IP connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number is 1492 byte
DNS	If ISP provides you DNS information, please select Attain DNS automatically , otherwise select Set DNS Manually and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP, default setting is internet .
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is *99# .
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	Select Enable Ping Access on WAN , will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to

	see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.1.3 WAN Access Type -- PPPoE

If you applied for a **PPPoE** connection type from ISP, please follow the steps to set up your WAN connection.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface: Ethernet Port

WAN Access Type: PPPoE

User Name:

Password:

Service Name:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1452 (1360-1492 bytes)

☒ Attain DNS Automatically

☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

3.5G Backup: ☒ Backup of connection, check connection in every 3 minutes

Service: UMTS/HSPA/HSDPA/HSUPA

Connect Speed: ☒ Auto Switch ☐ 2.5G/2.75G only ☐ 3G/3.5G only

SIM PIN: ☒ None

Retype SIM PIN:

APN: internet

User Name:

Password:

PHONE Number: *99#

Clone MAC Address: 000000000000

☒ Enable IGMP Proxy

☒ Enable Ping Access on WAN

☒ Enable Web Server Access on WAN

Item	Description
User Name	Input your user name supplied by ISP. If you don't know, please check with your ISP.

Password	Input your Password supplied by ISP
Service Name	Input the service name supplied by ISP.
Connection Type	It has three types: Continuous , Connect on Demand , and Manual .
Idle Time	It is the time of inactivity before disconnecting your PPPoE session. Enter an Idle Time (in minutes) to define a maximum period of time for which the Internet connect is maintained during inactivity. If the connection is inactive for longer than the defined Idle Time, then the connection will be dropped. Either set this to zero or enable Auto-reconnect to disable this feature.
MTU Size	MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed by Ethernet at the network layer is 1492 byte
DNS	If ISP provides you DNS information, please select Attain DNS automatically , otherwise select Set DNS Manually and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP,

	default setting is internet .
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is *99# .
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	Select Enable Ping Access on WAN , will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.1.4 WAN Access Type -- PPTP

If you have applied for a **PPTP** connection type from ISP, please follow the steps to set up your WAN connection.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface: Ethernet Port

WAN Access Type: PPTP

Address Mode: ☒ Dynamic ☐ Static

Server IP Address:

User Name:

Password:

MTU Size: (1400-1460 bytes)

☒ Attain DNS Automatically
☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

3.5G Backup: ☒ Backup of connection, check connection in every minutes.

Service: UMTS/HSPA/HSDPA/HSUPA

Connect Speed: ☒ Auto Switch ☐ 2.5G/2.75G only ☐ 3G/3.5G only

SIM PIN: ☒ None

Retype SIM PIN:

APN:

User Name:

Password:

PHONE Number:

Clone MAC Address:

☒ Enable IGMP Proxy
☒ Enable Ping Access on WAN
☒ Enable Web Server Access on WAN

Apply Change Reset

Item	Description
IP Address	Input your IP Address supplied by ISP. If you don't know, please check with your ISP.

Subnet Mask	Input Subnet Mask, normally it is 255.255.255.0 .
Server IP Address	Input your Server IP Address supplied by ISP. If you don't know, please check with your ISP.
User Name	Input the PPTP Account supplied by ISP, for example. If you don't know, please check with your ISP.
Password	Input the Password supplied by ISP.
MTU	MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed is 1460 byte
Request MPPPE Encryption	Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. 128-bit key (strong), 56-bit key, and 40-bit key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
DNS	If ISP provides you DNS information, please select Attain DNS automatically , otherwise select Set DNS Manually and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.

SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP, default setting is internet .
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is *99# .
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	Select Enable Ping Access on WAN , will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.1.5 WAN Access Type – L2TP

If you have applied for a **PPTP** connection type from ISP, please follow the steps to set up your WAN connection.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface: Ethernet Port

WAN Access Type: PPTP

Address Mode: ☒ Dynamic ☐ Static

Server IP Address:

User Name:

Password:

MTU Size: 1460 (1400-1460 bytes)

☒ Attain DNS Automatically
☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

☒ Enable IGMP Proxy
☐ Enable Ping Access on WAN
☐ Enable Web Server Access on WAN

Apply Change Reset

Item	Description
IP Address	Input your IP Address supplied by ISP. If you don't know, please check with your ISP.
Subnet Mask	Input Subnet Mask, normally it is 255.255.255.0 .
Server IP Address	Input your Server IP Address supplied by ISP. If you

	don't know, please check with your ISP.
User Name	Input the PPTP Account supplied by ISP, for example. If you don't know, please check with your ISP.
Password	Input the Password supplied by ISP.
MTU	MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed is 1460 byte
Request MPPPE Encryption	Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. 128-bit key (strong), 56-bit key, and 40-bit key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
DNS	If ISP provides you DNS information, please select Attain DNS automatically , otherwise select Set DNS Manually and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP,

	default setting is internet .
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is *99# .
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	Select Enable Ping Access on WAN , will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.2 WAN Interface – 3.5G (HSDPA/UMTS)

If you are using HSDPA/UMTS (3.5G connection) as the WAN Type, please select **3.5G USB Dongle** and fill in the required information as follows to directly access Internet via connected 3.5G adapter. At this moment, **Backup of Connection** is not available. When 3.5G signal cannot be reached, the system starts to search downward for 3G/2.75G/2.5G signals until none existed.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface:

3.5G usb dongle

Service:

UMTS/HSPA/HSDPA/HSUPA

Connect Speed:

☒ Auto Switch ☐ 2.5G/2.75G only ☐ 3G/3.5G only

SIM PIN:

☒ None

Retype SIM PIN:

APN:

internet

User Name:

Password:

PHONE Number:

*99#

☒ Attain DNS Automatically

☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

000000000000

☒ Always

☐ Dial on demand

Idle (0~60 Minutes, if input 0 or no input, it will set to Always mode)

☐ Manual

Connect

disconnect

☒ Enable IGMP Proxy

☒ Enable Ping Access on WAN

☒ Enable Web Server Access on WAN

Apply Change

Reset

Item	Description
Service	Select correspond mobile connection service type.
Connection Speed	Select preferred mobile Internet connection speed.
SIM PIN	Enter the PIN code of your SIM card here.
Retype SIM PIN	Confirm your PIN code.
APN	Enter the Access Point Number provided by your ISP. Default is internet .
Username	Username/Password required for establishing the Internet connection.
Password	
PHONE Number	Enter the dialing number here, default setting is *99# .
DNS	If ISP provides you DNS information, please select Attain DNS automatically , otherwise select Set DNS Manually and input the DNS information into the blank.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Always	Select Always for the 3.5G connection to be always established.
Dial on demand	Select Dial on demand to establish 3.5G connection only when there is an outgoing traffic.
Manual	Select Manual to manually connect or disconnect the 3.5G connection.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	Select Enable Ping Access on WAN , will make WAN IP address response to any ping request from Internet

	users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.3 WAN Access Type – WiMAX

If you are using WiMAX as the WAN Type, please select **WiMAX** and fill in the required information as follows to directly access Internet via connected WiMAX adapter.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface:

Operator:

User Name:

Password:

☒ Attain DNS Automatically
☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

☒ Enable IGMP Proxy
☒ Enable Ping Access on WAN
☒ Enable Web Server Access on WAN

Item	Description
Operator	Select Service Provider. (predefined, contents vary by region).
User Name	Enter your WiMAX user name here.
Password	Enter your password here.
DNS	If ISP provides you DNS information, please select Attain DNS automatically , otherwise select Set DNS Manually and input the DNS information into the

	blank.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable IGMP Proxy to provide service.
Enable Ping Access on WAN	Select Enable Ping Access on WAN , will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.1.4 WAN Access Type – Wireless

If you are connecting the internet via wireless, please select **Wireless** and its associated settings will show up underneath at the same time.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Interface: Wireless

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
CBR-980	00:d0:41:b9:e2:9d	11 (B+G+N)	AP	no	64	<input checked="" type="radio"/>

Encryption: None Refresh

WAN Access Type: DHCP Client

Host Name: default

MTU Size: 1492 (1400-1492 bytes)

☒ Attain DNS Automatically

☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

☒ Enable IGMP Proxy

☐ Enable Ping Access on WAN

☐ Enable Web Server Access on WAN

Apply Change Reset

You can see a list of available Wireless networks. Select you preferred one to connect and the Encryption type form the drop-down list.

4.1.2 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your router. Here you may change the setting for IP address, subnet mask, DHCP, etc.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="button" value="Server"/> <input type="button" value="v"/>
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
Static DHCP:	<input type="button" value="Set Static DHCP"/>
Device Name:	<input type="text" value="CQR-981"/>
802.1d Spanning Tree:	<input type="button" value="Disabled"/> <input type="button" value="v"/>
Clone MAC Address:	<input type="text" value="000000000000"/>

Item	Description
IP Address	The default IP address is 192.168.1.1
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Please enter the Default Gateway address for LAN interface.
DHCP	Click to select Disabled , Client or Server in different operation mode of LAN access point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range
Static DHCP	Configures how static DHCP address are assigned to client (only available when DHCP server is enabled)
Device Name	Configures the device name of the router.
802.1d Spanning Tree	IEEE 802.1d Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. Select enable or disable the IEEE 802.1d Spanning Tree function from

	pull-down menu.
Clone MAC Address	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.1.3 Dynamic DNS Setting

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

Note: make sure that you have registered with a DDNS service provider before enabling this feature.

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☐ Enable DDNS

Service Provider :

DynDNS

Domain Name :

User Name/Email:

Password/Key:

Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)
For DynDNS, you can create your DynDNS account [here](#)

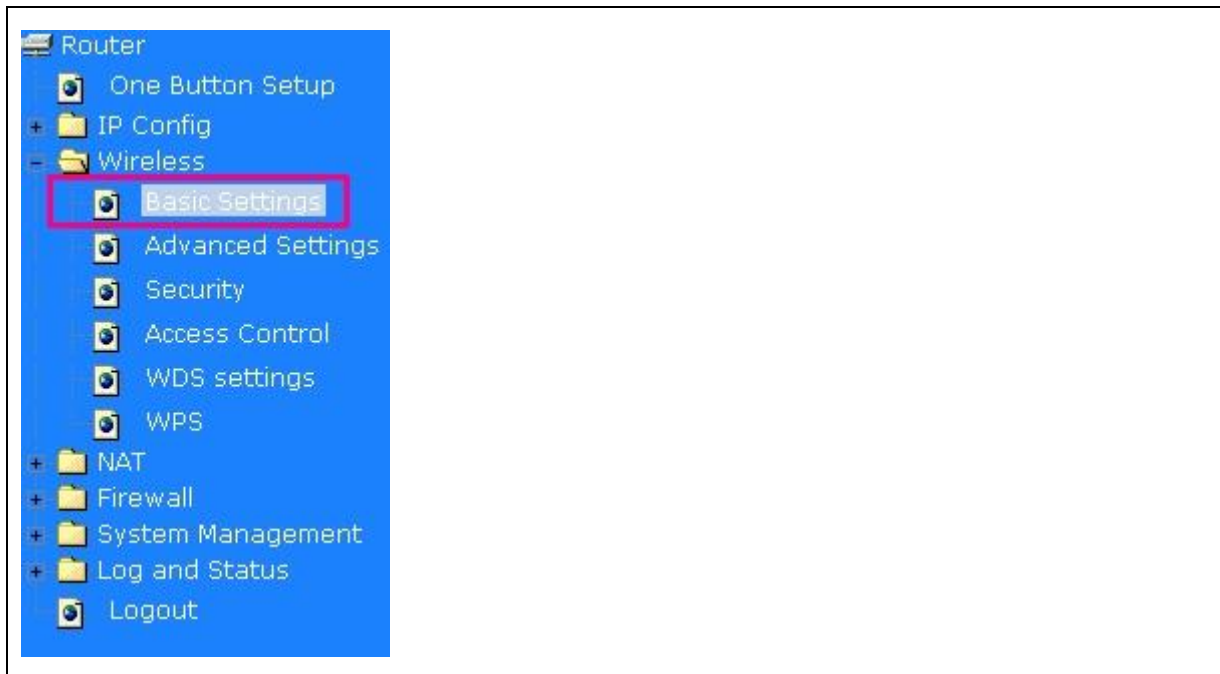
Please select a DDNS Service Provider

Please enter **Domain Name**, **User Name/Email**, and **Password/Key**. After entering, click on **Apply Changes** to save the setting, or you may click on **Reset** to clear all the input data.

Item	Description
Enable/Disable DDNS	Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.
Service Provider	Choose correct Service Provider from drop-down list, here including DynDNS, TZO, ChangeIP, Eurodns, OVH, NO-IP, ODS, Regfish embedded in CQR-981.
User Name/Email	User name is used as an identity to login Dynamic-DNS service.
Password/Key	Password is applied to login Dynamic-DNS service.
Apply & Cancel	Click on Apply button to continue. Click on Cancel button to clear the setting on this page.

4.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Security**, **Access Control**, **WDS settings**, and **WPS**. Please read below for the setting instruction.



4.2.1 Wireless Basic Settings

The Wireless Basic Settings include Band, Mode, SSID, Channel Number and other wireless settings.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G+N) ▼

Mode: AP ▼

Multiple AP

Network Type: Infrastructure ▼

SSID: CQR-981

Channel Width: 40MHz ▼

Control Sideband: Upper ▼

Channel Number: 6 ▼

Broadcast SSID: Enabled ▼

WMM: Enabled ▼

Data Rate: Auto ▼

Associated Clients: Show Active Clients

☐ **Enable Mac Clone (Single Ethernet Client)**

☐ **Enable Universal Repeater Mode (Acting as AP and client simultaneously)**

SSID of Extended Interface: ESSID_CQR-981

Apply Change

Reset

Item	Description
Disable Wireless LAN Interface	Turn off the wireless service.
Band	Please select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	Please select the mode. It has 3 modes to select:(AP, Client, WDS, AP+WDS). Multiple APs provides users another 4 different SSID for connection. Users can add or limit the properties for each connection. Please check Section 4.2.1.1
SSID	Service Set identifier, the default SSID is CNet , users can define to any.
Channel Width	Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.
Channel Number	Please select the channel; it has Auto, 1, 2~11 or 13 options.
Broadband SSID	User may choose to enable Broadcast SSID or not.
Data Rate	Please select the data transmission rate.
Associate Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
Enable Universal Repeater Mode (Acting as AP and Client simultaneously)	Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.) Please check Section 4.2.1.2
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.2.1.1 Multiple APs

Multiple APs provides users another 4 different SSIDs for connection. Each SSID could be set with different data rate, WMM and access type.

Multiple APs

This page shows and updates the wireless setting for multiple APs.

No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_1	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show
AP2	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_2	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show
AP3	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_3	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show
AP4	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_4	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show

Apply ChangeResetClose

Item	Description
Enable	Enable or disable the service.
Band	Select the frequency.
SSID	Enter the SSID.
Data Rate	Select the data transmission rate.
Access	Enable this function can let clients use two access types: a. LAN+WAN: the client can access to the Internet and access in the router's GUI. b. WAN: the client can only access to the Internet.
Active Client List	Display the properties of the client which is connecting successfully.
Apply Changes	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.2.1.2 Enable Universal Repeater Mode (Acting as AP Client simultaneously)

The router can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.

Example: When users enable the Universal Repeater to connect to the upper level device, please fill in the upper level device's channel and SSID. Click on **Apply Changes** to save the settings.
(Please disable the DHCP service first)

The screenshot shows a configuration page for the Universal Repeater Mode. Several elements are highlighted with red rectangular boxes:

- Channel Number:** A dropdown menu showing the value '6'.
- Broadcast SSID:** A dropdown menu showing the value 'Enabled'.
- WMM:** A dropdown menu showing the value 'Enabled'.
- Data Rate:** A dropdown menu showing the value 'Auto'.
- Associated Clients:** A button labeled 'Show Active Clients'.
- Enable Mac Clone (Single Ethernet Client):** An unchecked checkbox.
- Enable Universal Repeater Mode (Acting as AP and client simultaneously):** A checked checkbox.
- SSID of Extended Interface:** A text input field containing the value 'ESSID_CQR-981'.
- Apply Change:** A button at the bottom left.
- Reset:** A button at the bottom right.

Users can use the Network Configuration page to check the information about “**Wireless Repeater Interface Configuration**”.

Router

One Button Setup

IP Config

Wireless

NAT

Firewall

System Management

Log and Status

Network Config

Event Log

Logout

Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:2h:33m:5s
Firmware Version	Ver1.0.2
WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CQR-981
Channel Number	6
Encryption	Disabled
MAC Address	00:08:a1:c7:a5:2b
Associated Clients	1
WirelessRepeater Interface Configuration	
Mode	Infrastructure Client
ESSID	ESSID_CQR-981
Encryption	Disabled
MAC Address	00:00:00:00:00:00
State	Scanning

4.2.2 Wireless Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Preamble Type: ☒ Long Preamble ☐ Short Preamble

IAPP: ☒ Enabled ☐ Disabled

Protection: ☐ Enabled ☒ Disabled

Aggregation: ☒ Enabled ☐ Disabled

Short GI: ☒ Enabled ☐ Disabled

WLAN Partition: ☐ Enabled ☒ Disabled

RF Output Power: ☒ 100% ☐ 70% ☐ 50% ☐ 35% ☐ 15%

Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.
Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol

	data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and 15%.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.2.3 Wireless Security Setup

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link.** There are five Encryption types supported: "None", "WEP", "WPA (TKIP)", "WPA2(AES)", and "WPA2 Mixed".

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - CQR-981 ▼ Apply Change Reset

Encryption: Disable ▼

802.1x Authentication: ☐

1. Encryption -- WEP Key

1.1 Set WEP Key: This section provides 64bit and 128bit WEP encryptions and two different shared key formats (ASCII and Hex) for wireless network.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - CQR-981 ▼ Apply Change Reset

Encryption: WEP ▼

802.1x Authentication: ☐

Authentication: ☐ Open System ☐ Shared Key ☒ Auto

Key Length: 64-bit ▼

Key Format: Hex (10 characters) ▼

Encryption Key: *****

802.1x Authentication: It is a safety system by using authentication to protect your wireless network.

2. Encryption – WPA (WPA, WPA2, and WPA2 Mixed), WPA Authentication Mode

- Enterprise (RADIUS): Please fill in the RADIUS server Port, IP Address, and Password

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode:

☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite:

☐ TKIP ☐ AES

Pre-Shared Key Format:

Pre-Shared Key:

- Personal (Pre-Shared Key): Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode:

☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite:

☐ TKIP ☐ AES

WPA2 Cipher Suite:

☐ TKIP ☒ AES

Pre-Shared Key Format:

Pre-Shared Key:

3. Apply Change & Reset: Click on '**Apply Changes**' to save setting data. Or click '**Reset**' to reset all the input data.

4.2.4 Wireless Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on “Apply Changes” to save the new addition. To delete a MAC address, select its corresponding checkbox under the **Select** column and click on “Delete Selected” button.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable ▾

MAC Address: Comment:

Apply Changes Reset

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected Delete All Reset

Take the wireless card as the example.

- (1) Here is the example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then fill in the MAC address what you plan to block in the MAC Address field. Click **Apply Changes** to save the setting.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Deny Listed ▼

MAC Address: 0018F8638A54

Comment:

Apply Change

Reset

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

(2) The MAC address what you set will be displayed on the **Current Access Control List**.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Deny Listed ▼

MAC Address:

Comment:

Apply Change

Reset

Current Access Control List:

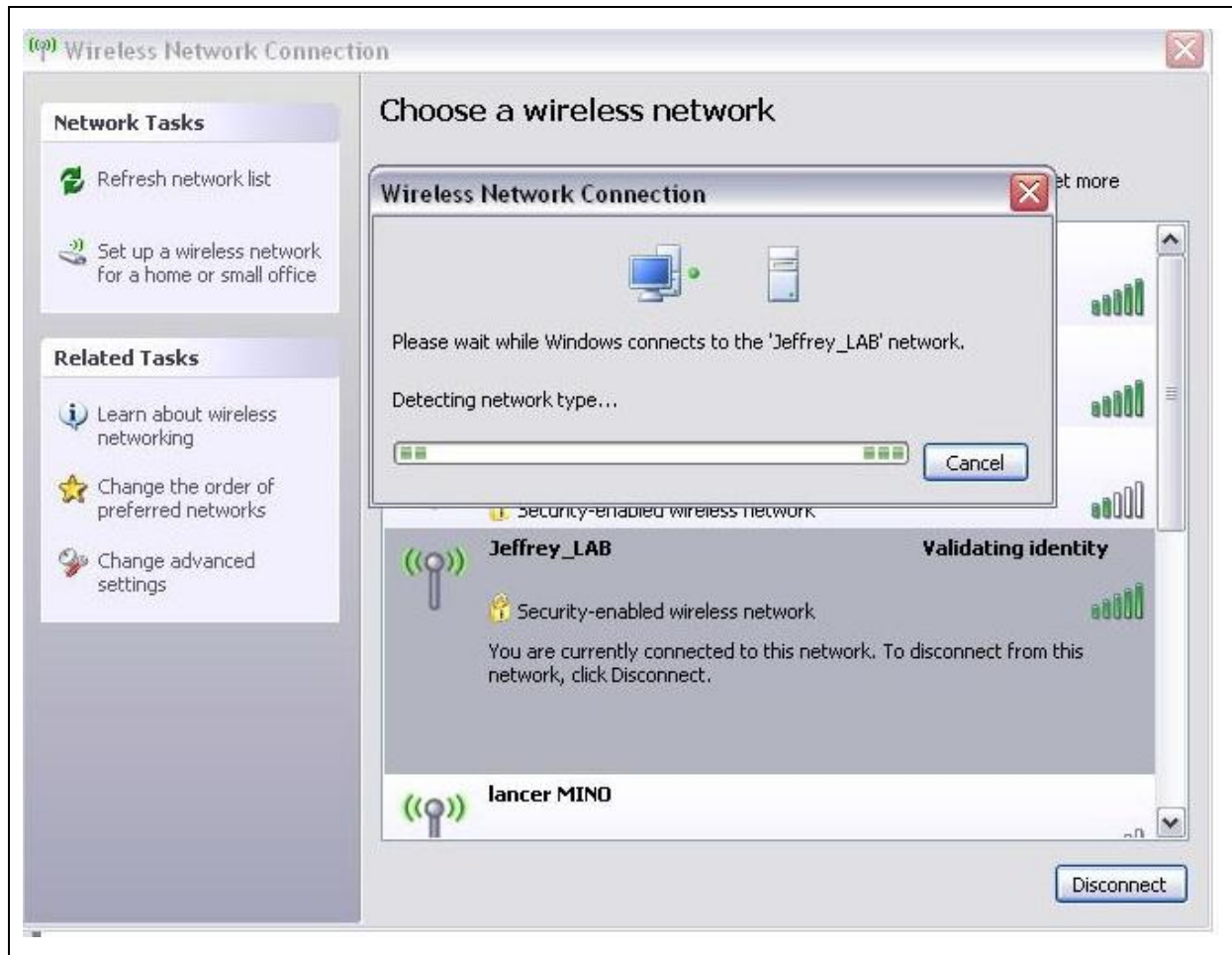
MAC Address	Comment	Select
00:18:f8:63:8a:54		<input type="checkbox"/>

Delete Selected

Delete All

Reset

(3) The wireless client will be denied by the wireless router.



4.2.5 WDS Settings

When selected in the Basic Settings page and enabled here, Wireless Distribution System (WDS) enables the router to be used as a wireless bridge. Two Wireless-G Routers in bridge mode can communicate with each other through their wireless interfaces. To accomplish this, all wireless routers should be set to the same channel and the MAC address of other AP / Routers should be entered in the table.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☐ **Enable WDS**

MAC Address:

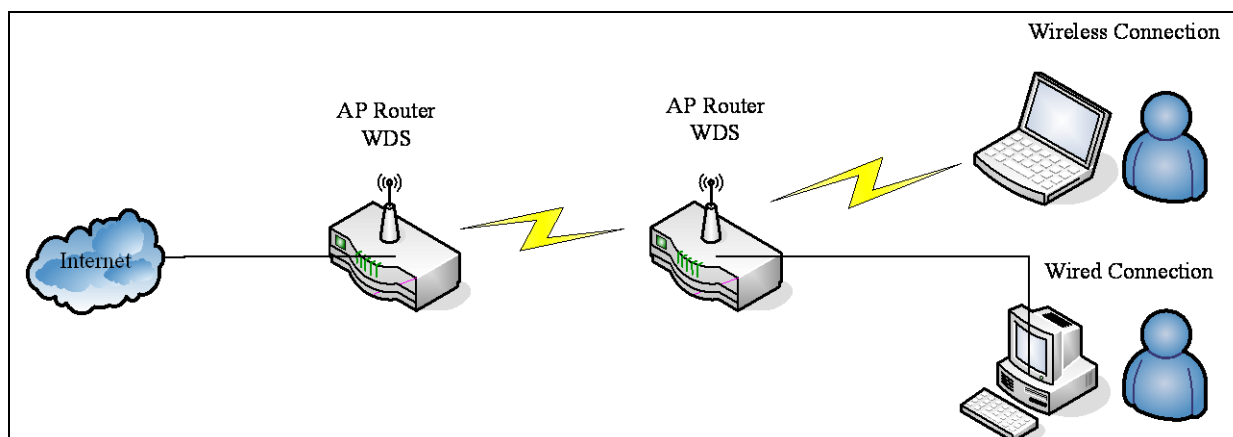
Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

The WDS explanation as the following picture.



*Please follow the below instructions to setup the WDS connection.

(1) Please check the MAC address and Channel number from the upper lever device.

Network Config	
This page shows the current status and some basic settings of the device.	
System	
Uptime	1day:3h:2m:45s
Firmware Version	Ver1.0.1
WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CNet
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:96:b1
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:b1

- (2) Set the connection mode to “AP+WDS” from “Wireless Basic Setting”, and then select the channel number(in this example is “11”). Click **Apply Changes** to save the setting.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:

2.4 GHz (B+G+N) ▾

Mode:

AP+WDS ▾

Multiple AP

Network Type:

Infrastructure ▾

SSID:

CNet

Channel Width:

40MHz ▾

Control Sideband:

Upper ▾

Channel Number:

11 ▾

Broadcast SSID:

Enabled ▾

WMM:

Enabled ▾

Data Rate:

Auto ▾

Associated Clients:

Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

ESSID_Cnet

Apply Change

Reset

- (3) Enable WDS function from the page – “WDS Setting”, and then fill in the upper level device MAC address. Click **Apply Changes** to save the setting data.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☒ **Enable WDS**

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

- (4) The WDS AP List will show the WDS device MAC address after reboot.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☒ **Enable WDS**

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:0e:68:ff:05:c8	Auto		<input type="checkbox"/>

(5) Set "Broadcast SSID" to disable from page "Wireless Basic Setting".

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:

2.4 GHz (B+G+N) ▾

Mode:

AP+WDS ▾

Multiple AP

Network Type:

Infrastructure ▾

SSID:

CNet

Channel Width:

40MHz ▾

Control Sideband:

Upper ▾

Channel Number:

11 ▾

Broadcast SSID:

Enabled ▾

WMM:

Enabled ▾

Data Rate:

Auto ▾

Associated Clients:

Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

ESSID_Cnet

Apply Change

Reset

(6) Go to the upper level device WDS setting page and fill in the MAC address

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☒ **Enable WDS**

MAC Address:

Data Rate:

Comment:

Please input the MAC address of this router.

Apply Changes

Reset

Set Security

Show Statistics

Current WDS AP List:

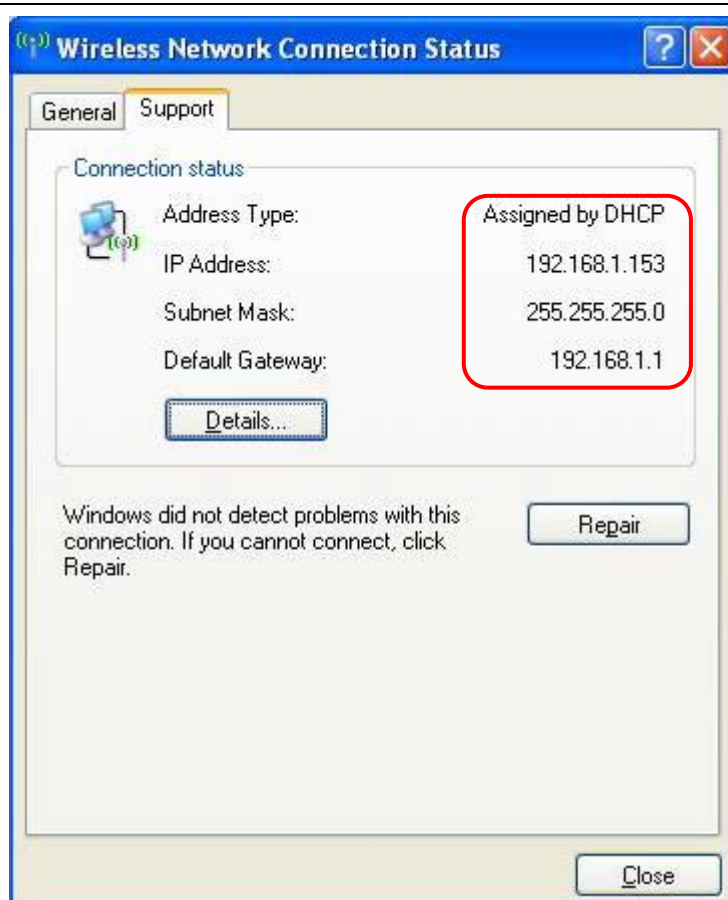
MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

Delete Selected

Delete All

Reset

(7) You will receive an IP address from the upper lever device.



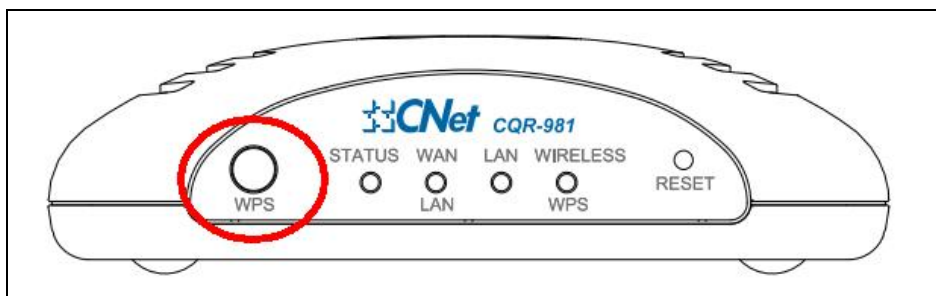
4.2.6 WPS

This page allows user to change the setting for WPS (*Wi-Fi Protected Setup*). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle. CQR-981 could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.

PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

Please find the WPS button from the following illustrate



When users select a specific model on wireless base station, the clients can connect to the base by selecting the same model.

The connection procedures of PIN and PBC are almost the same. The small difference between those two is:

Users input the PIN of wireless card in the base station first; it will limit the range of the clients. It is faster to establish a connection on PIN model.

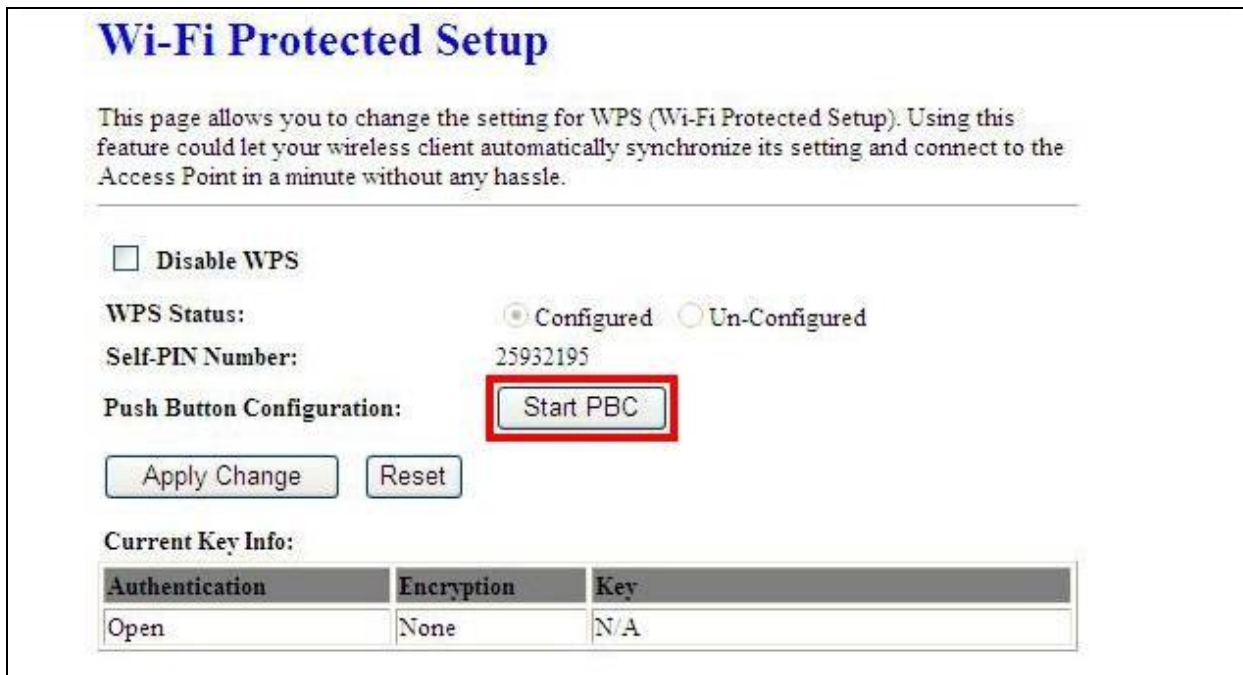
On PBC model, users push the WPS button to activate the function, and then the wireless client must push the WPS button in 2 minutes to enter the network. The client will search to see if there is any wireless base station which supports WPS is activating. If the client finds a matching base, the connection will be established. The speed of establishing a connection is slower than the PIN model because of this extra step.

On the other hand, users need to input the information of the wireless card into the register interface. It might lead to the failure of connection, if users make mistakes on inputting. On PBC model, users only need to click the WPS button on both sides to make a connection. It is easier to operate.

This page supports **Start PBC** and **Start PIN**; please read the following instructions

* Start PBC:

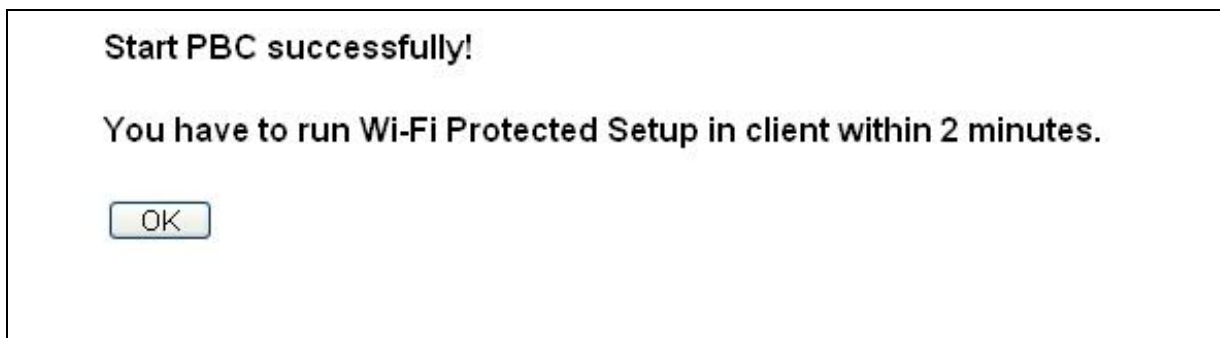
(1) Click **Start PBC** to connect to the wireless network card.



The image shows a web interface titled "Wi-Fi Protected Setup". It contains a description of the feature, a checkbox to "Disable WPS", and radio buttons for "WPS Status" (Configured and Un-Configured). The "Self-PIN Number" is displayed as 25932195. Under "Push Button Configuration", there is a "Start PBC" button highlighted with a red rectangle. Below this are "Apply Change" and "Reset" buttons. At the bottom, a section titled "Current Key Info:" contains a table with columns for Authentication, Encryption, and Key.

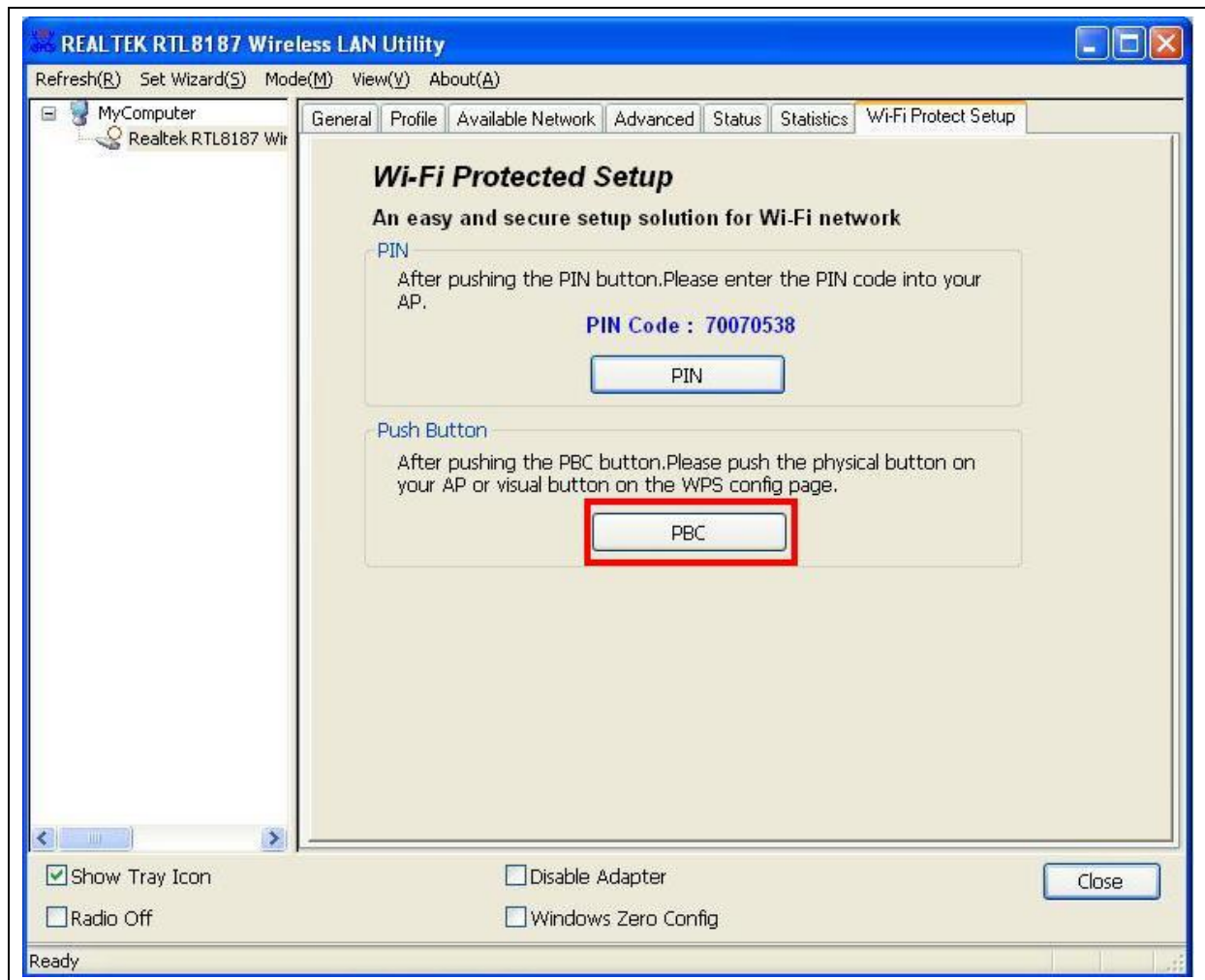
Authentication	Encryption	Key
Open	None	N/A

(2) Click **OK** to start WPS process.

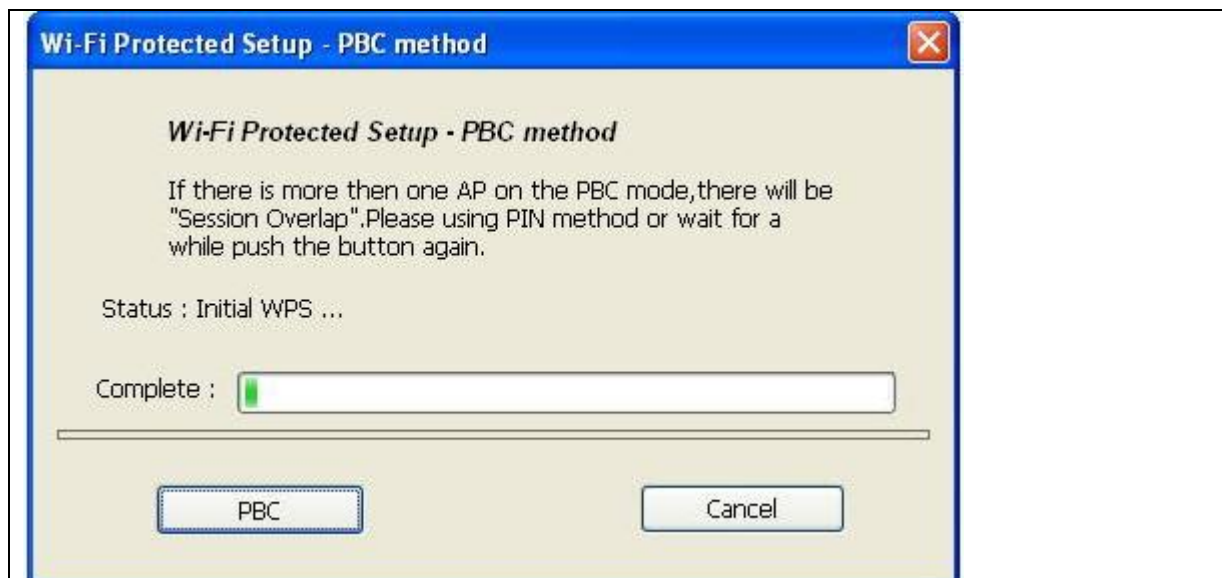


The image shows a dialog box with the title "Start PBC successfully!". The main text reads "You have to run Wi-Fi Protected Setup in client within 2 minutes." At the bottom, there is an "OK" button.

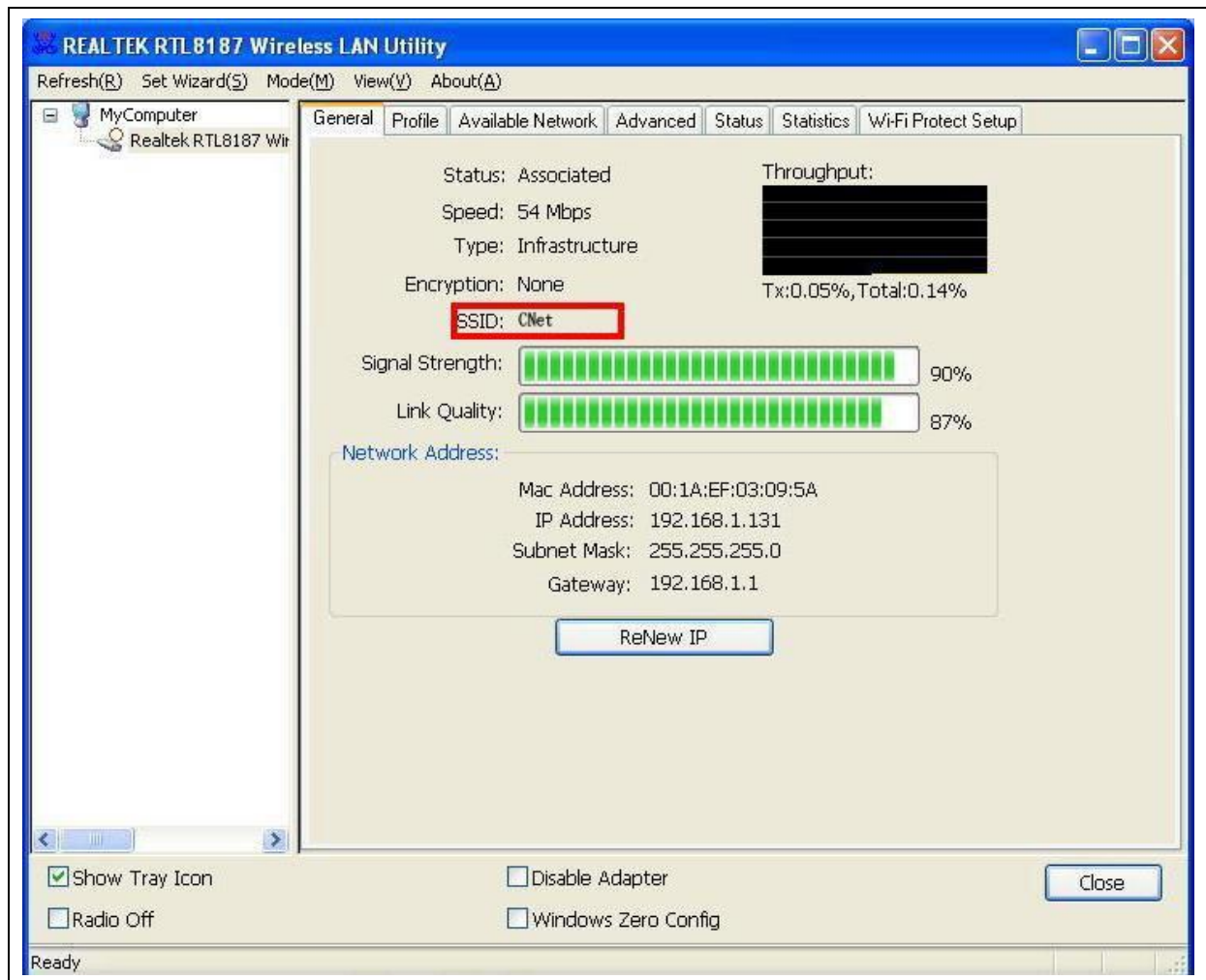
(3) Open the configuration page of the wireless card. Click the **Wi-Fi Protect Setup**, and then click **PBC** to start the WPS process.



(4) The WPS is being processed.

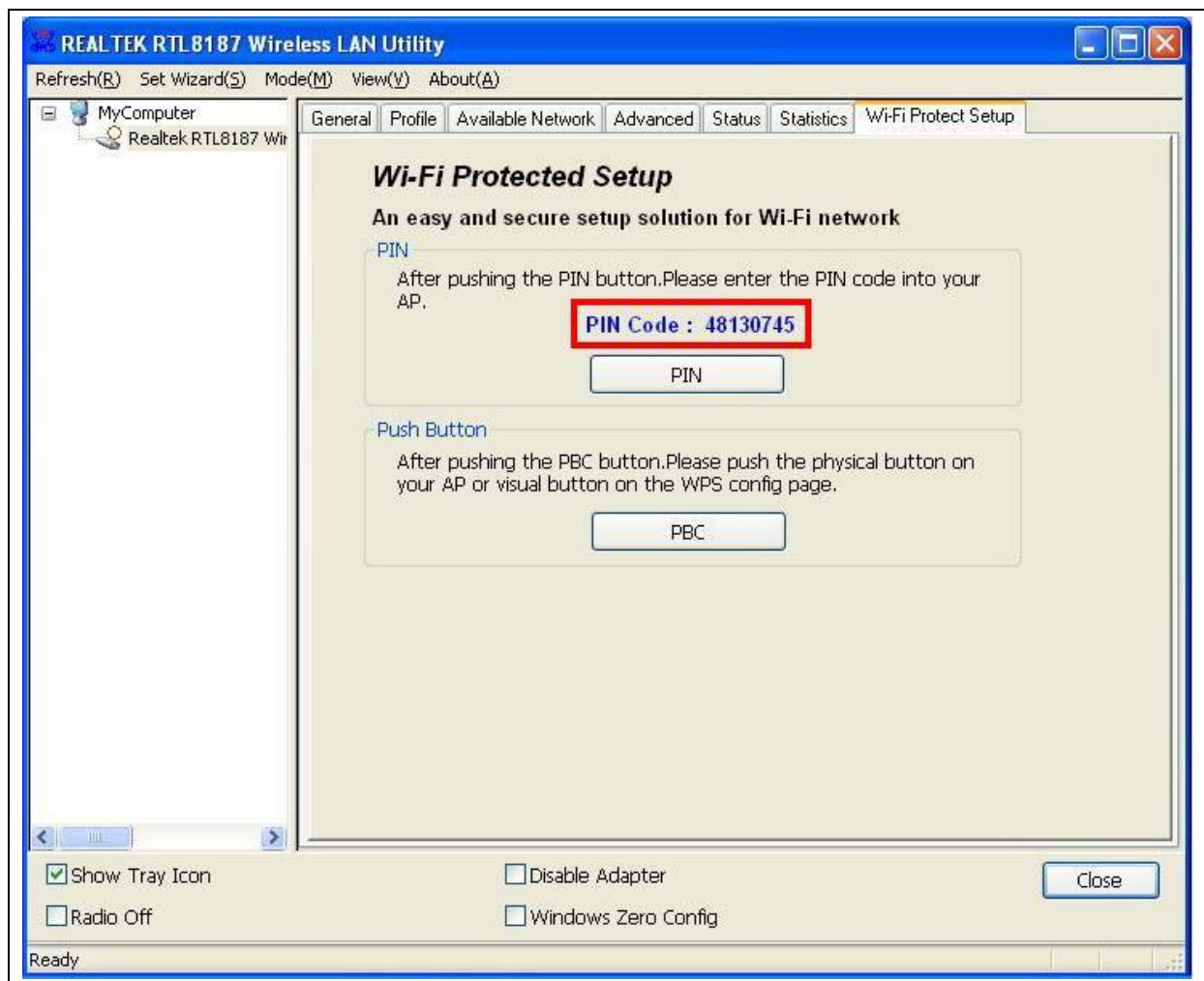


- (5) The USB dongle will receive the connection information from wireless router if the dongle has connected to the wireless router successfully.

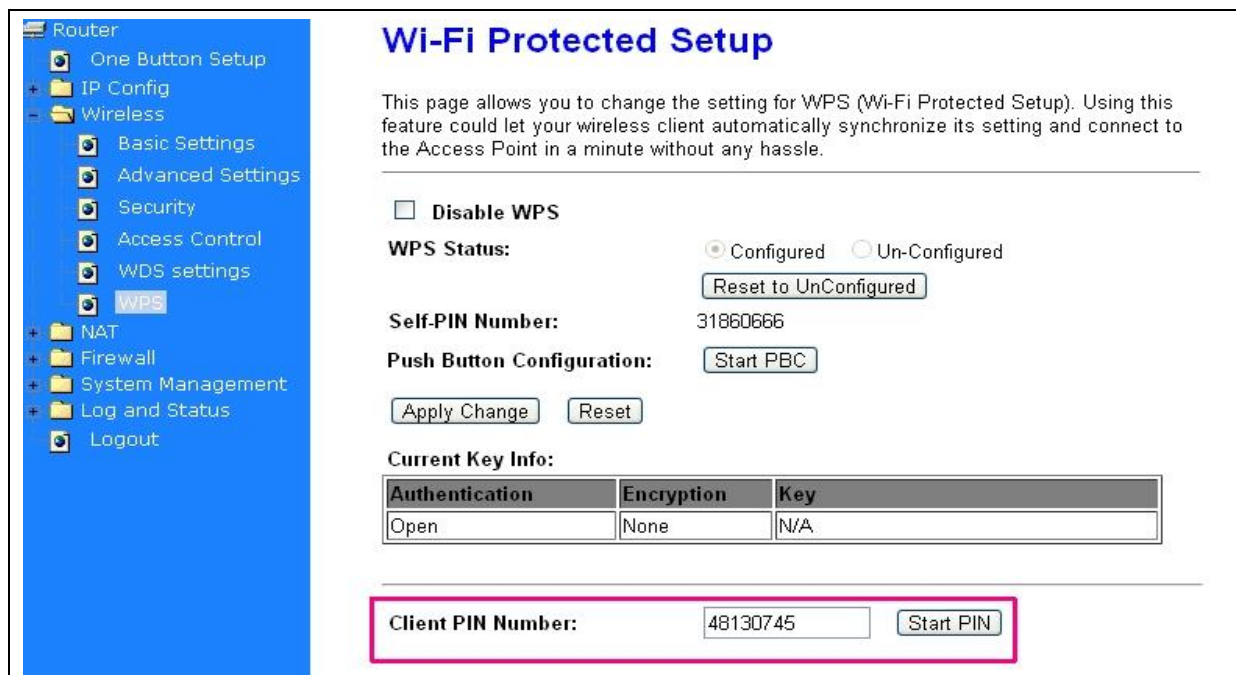


* Start PIN:

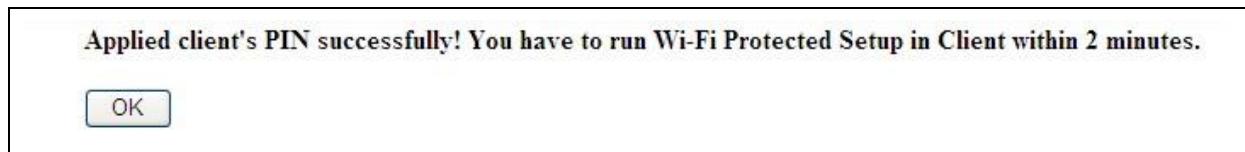
- (1.) Get the WPS PIN number from wireless card and write it down.



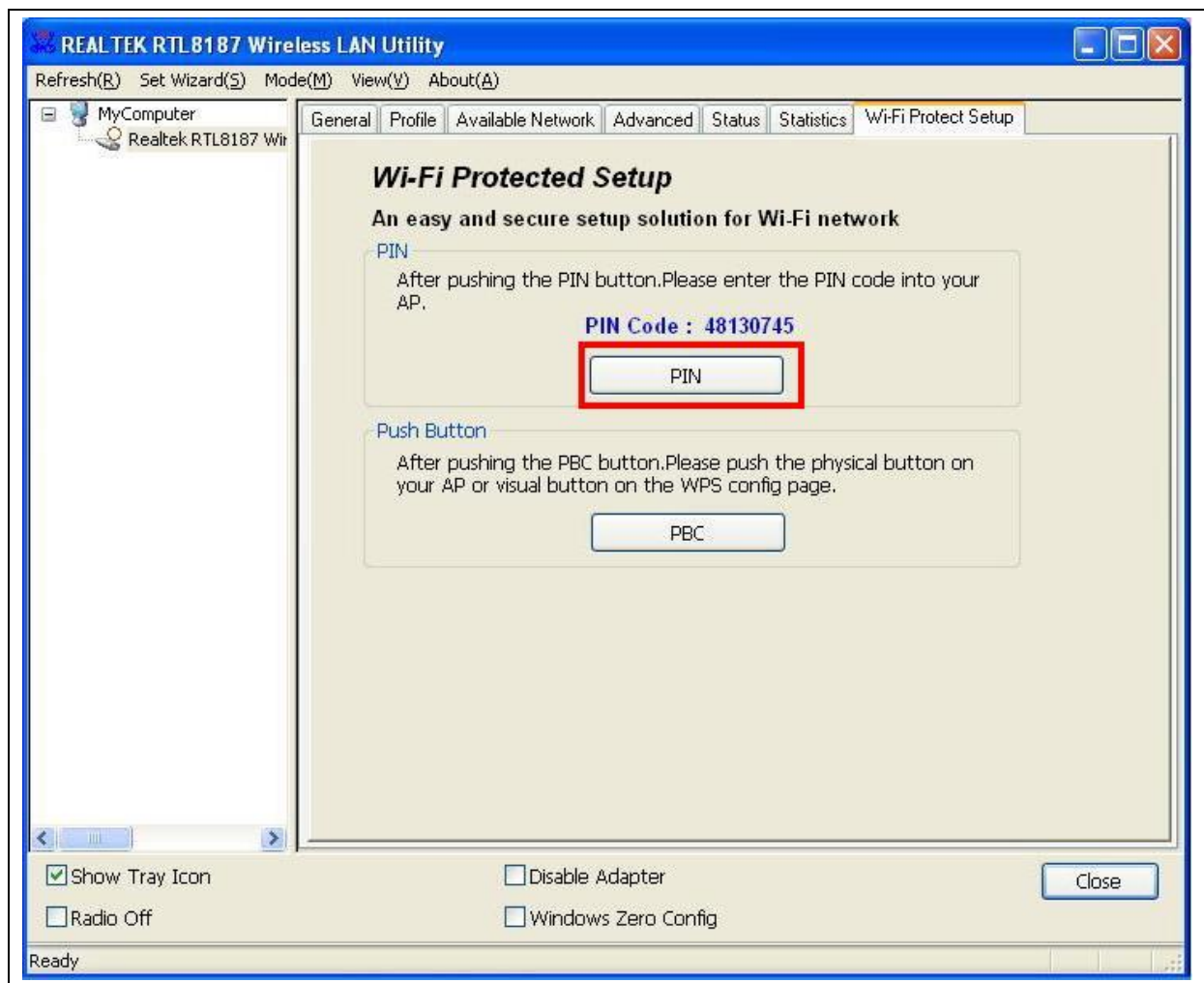
(2) Fill in the PIN number from the wireless card in Client PIN Number field, and then click “Start PIN”.



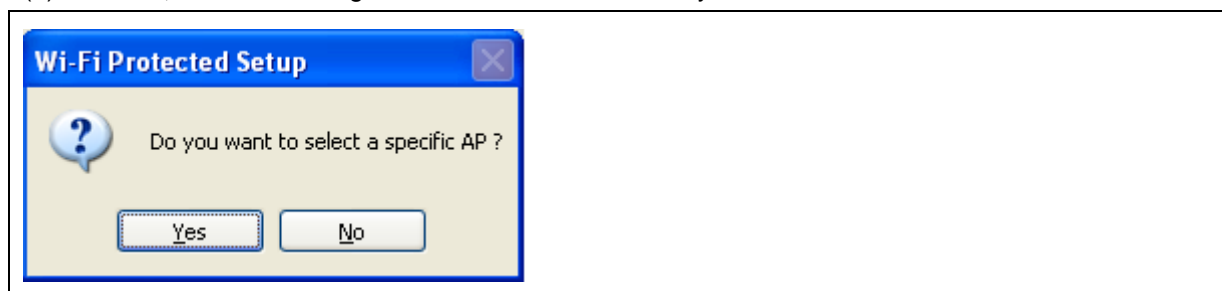
(3) Click **OK** to starts process.



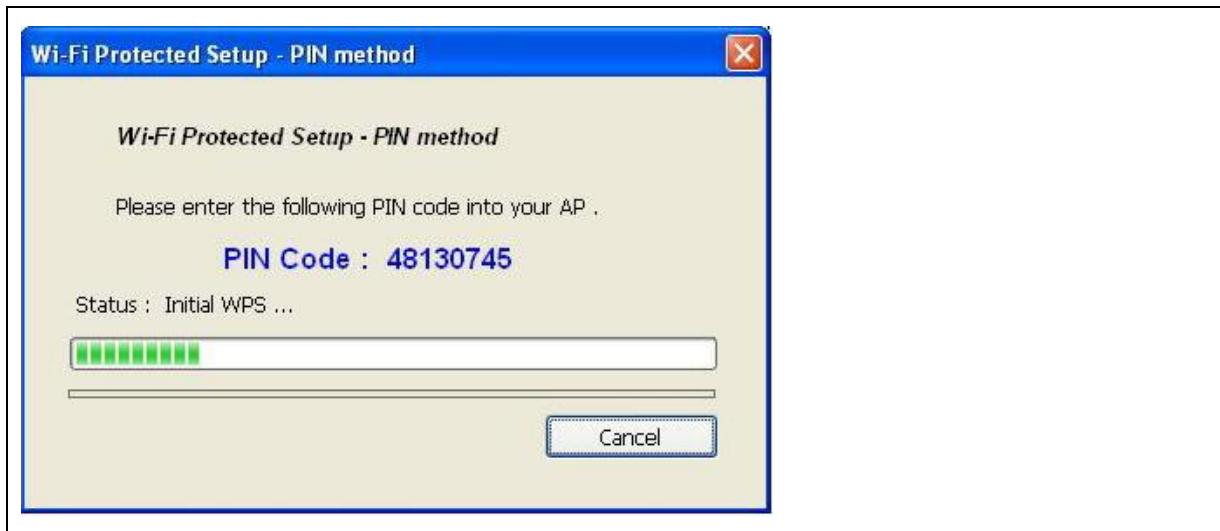
(4) Click **PIN** to start the WPS process with the wireless router.



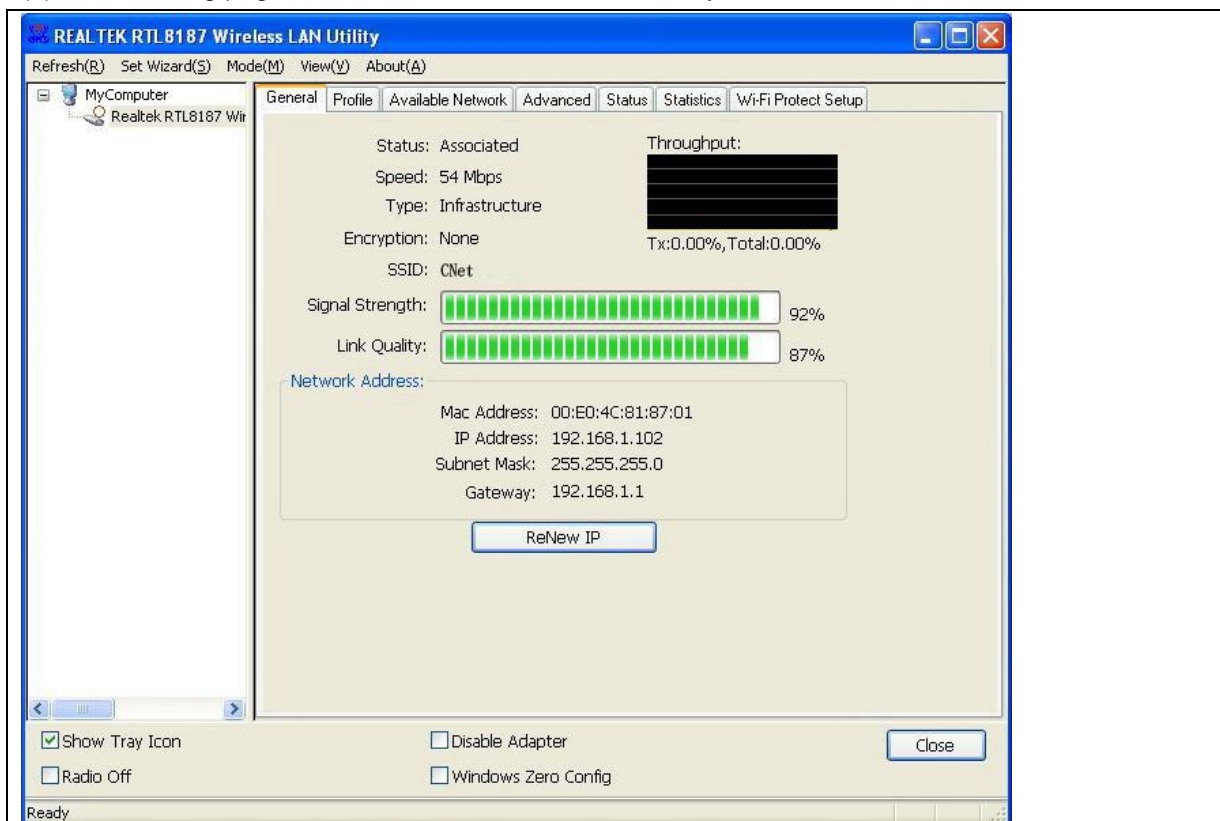
(5) Click **No**, then USB Dongle will select AP automatically.



(6) WPS is in processing.



(7) The following page shows the wireless card has already connected to the wireless router.



4.3 NAT

4.3.1 Virtual Server

The Virtual Server feature allows users to create Virtual Servers by re-directing a particular range of service port numbers (from the WAN port) to a particular LAN IP address.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ **Enable Port Forwarding**

Address : Protocol: Both ▾

Public Port Range: - Private Port:

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Public Port Range	Private Port	Comment	Select
------------------	----------	-------------------	--------------	---------	--------

Item	Description
Enable Port Forwarding	Select to enable Port Forwarding service or not.
IP Address	Specify the IP address which receives the incoming packets.
Protocol	Select the protocol type.
Port Range	Enter the port number, for example 80-80 or 20-22
Comment	Add comments for this port forwarding rule.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Port Forwarding Table	It will display all port forwarding regulation you made.
Delete Selected & Delete All	Click Delete Selected will delete the selected item. Click Delete All will delete all items in this table.
Reset	Click Reset to cancel.

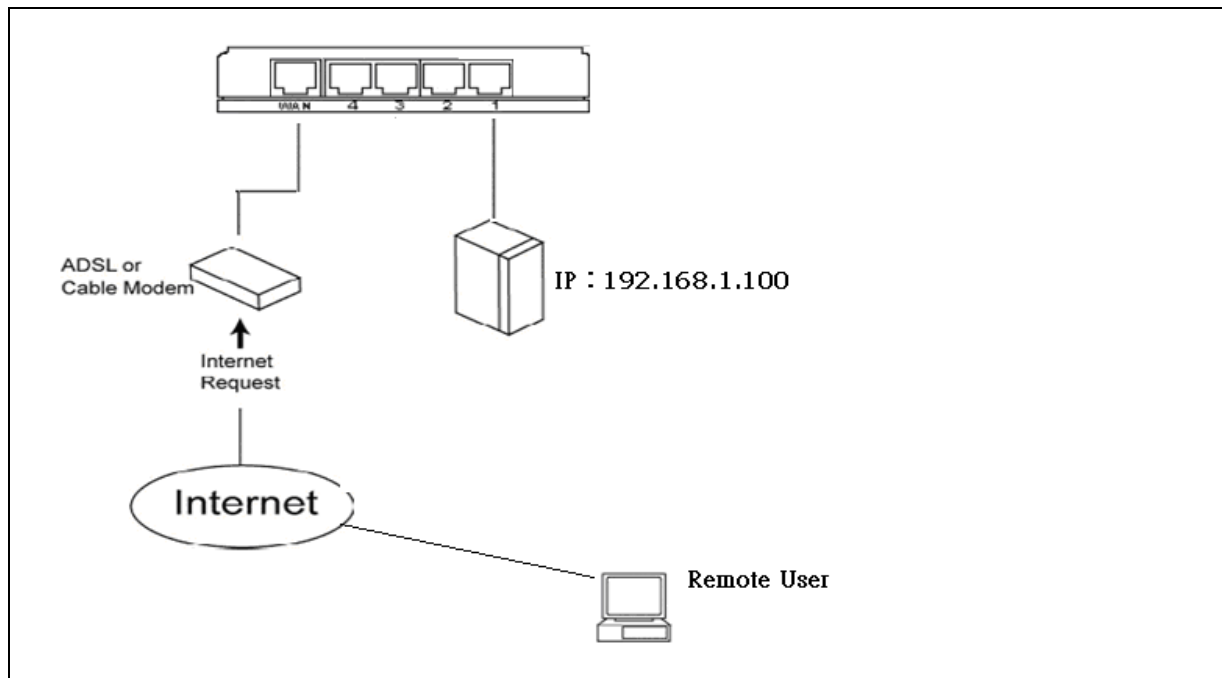
*Please find the following figure to know that what the virtual server is. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.

Configuration:

Private IP: 192.168.1.100

Port: 80 - 80

Type: TCP+UDP



4.3.2 DMZ

The DMZ feature allows one local user to be exposed to the Internet for special-purpose applications like Internet gaming or videoconferencing. When enabled, this feature opens all ports to a single station and hence renders that system exposed to intrusion from outside. The port forwarding feature is more secure because it only opens the ports required by that application.

Router

- One Button Setup
- + IP Config
- + Wireless
- NAT
 - Virtual Server
 - DMZ
- + Firewall
- + System Management
- + Log and Status
- Logout

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

☐ **Enable DMZ**

DMZ Host IP Address:

Item	Description
Enable DMZ	It will enable the DMZ service if you select it.
DMZ Host IP Address	Please enter the specific IP address for DMZ host.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

4.4 Firewall

Router

- One Button Setup
- + IP Config
- + Wireless
- + NAT
- **Firewall**
 - Port Filtering
 - IP Filtering
 - MAC Filtering
 - URL Filtering
- + System Management
- + Log and Status
- Logout

4.4.1 Port Filtering

When enabled packets are denied access to Internet/filtered based on their port address.

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable Port Filtering**

Port Range: - Protocol: Both Comment:

Current Filter Table:

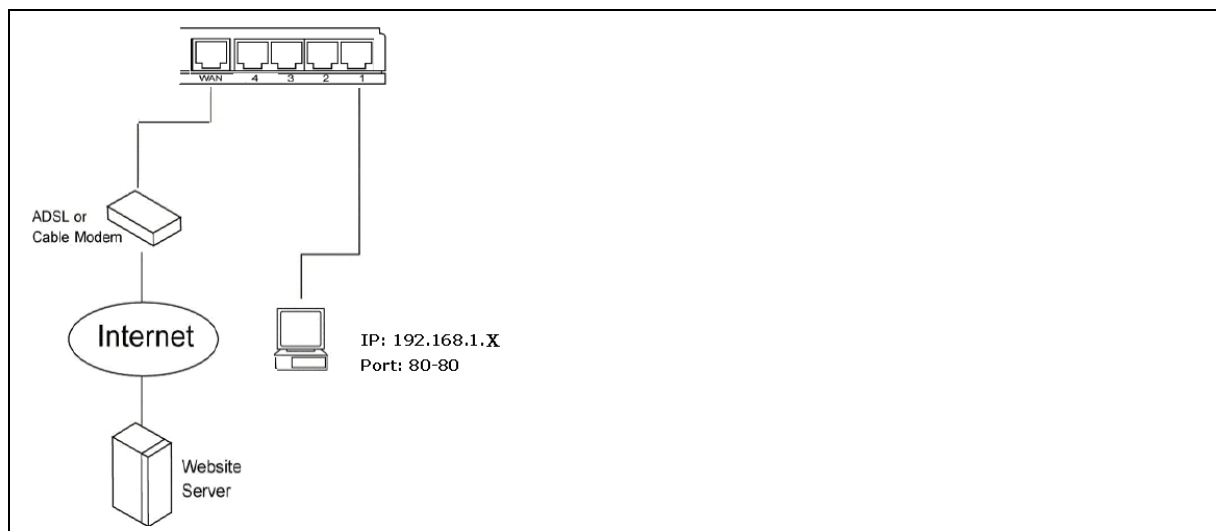
Port Range	Protocol	Comment	Select
------------	----------	---------	--------

Item	Description
Enable Port Filtering	Please select Enable Port Filtering to filter ports.
Port Range	Please enter the port number that needs to be filtered.
Protocol	Please select the protocol type of the port.
Comment	You can add comments for this regulation.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click Delete Selected will delete the selected item. Click Delete All will delete all items in this table.
Rest	You can click Reset to cancel.

* Port 80 has been blocked as the following illustrate.

IP: 192.168.1.X

Port: 80-80



4.4.2 IP Filtering

When enabled, LAN clients are blocked / filtered from accessing the Internet based on their IP addresses.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable IP Filtering**

Local IP Address: Protocol: Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Item	Description
Enable IP Filtering	Please select Enable IP Filtering to filter IP addresses.
Local IP Address	Please enter the IP address that needs to be filtered.
Protocol	Please select the protocol type of the IP address.
Comment	You can add comments for this regulation.

Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click Delete Selected will delete the selected item. Click Delete All will delete all items in this table.
Rest	You can click Reset to cancel.

4.4.3 MAC Filtering

When enabled, filtering will be based on the MAC address of LAN computers. Any computer with its MAC address on this list will be blocked from accessing the Internet.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable MAC Filtering

MAC Address:
Comment:

Current Filter Table:

MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>		

Item	Description
Enable MAC Filtering	Please select Enable MAC Filtering to filter MAC addresses
MAC Address	Please enter the MAC address that needs to be filtered.
Comment	You can add comments for this regulation.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click Delete Selected will delete the selected item. Click Delete All will delete all items in this table.
Rest	You can click Reset to cancel.

4.4.4 URL Filtering

URL Filtering is used to restrict users to access specific websites in internet

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☐ **Enable URL Filtering**

URL Address:

Current Filter Table:

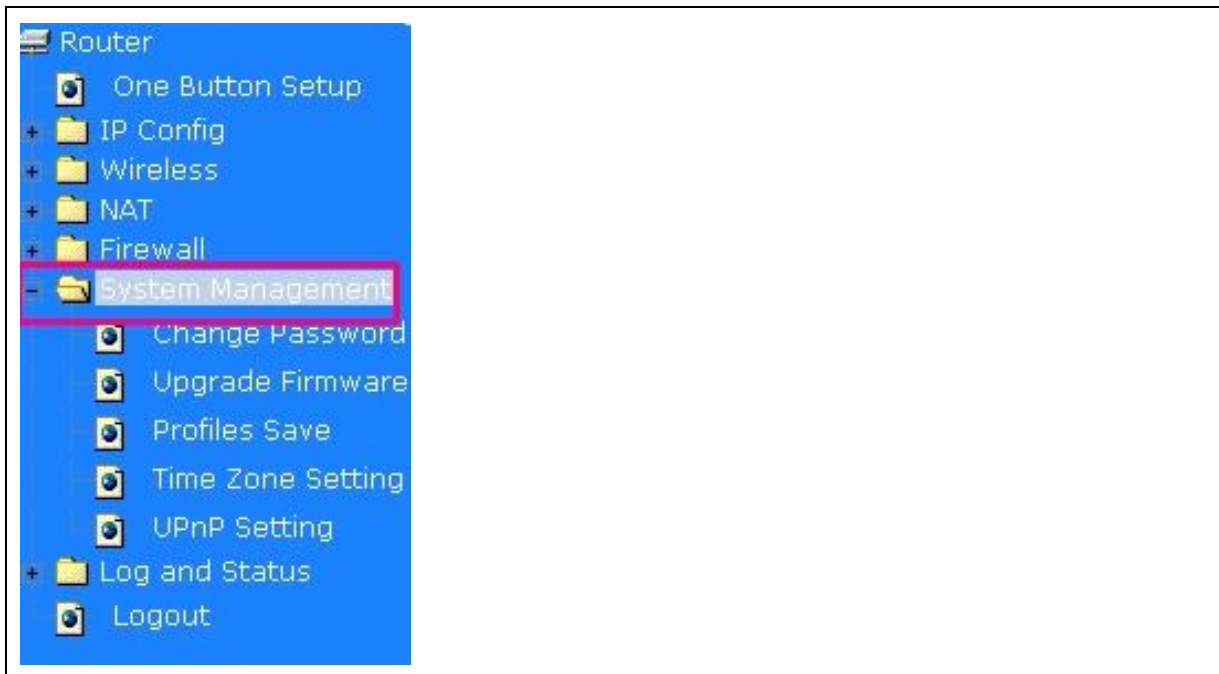
URL Address	Select
-------------	--------

Item	Description
Enable URL Filtering	Please select Enable MAC Filtering to filter MAC addresses
URL Address	Please enter the MAC address that needs to be filtered.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click Delete Selected will delete the selected item. Click Delete All will delete all items in this table.
Rest	You can click Reset to cancel.

Notes: This function will not be in effect when the Virtual Server is enabled. Please disable Virtual Server before activate the URL Filtering function.

4.5 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.



4.5.1 Change Password

Users can set or change user name and password used for accessing the web management interface in this section.

A screenshot of the 'Change Password' page in the router's web management interface. The left sidebar is the same as the previous image, with 'System Management' and 'Change Password' highlighted with red boxes. The main content area has the title 'Change Password' in blue. Below the title is a warning: 'This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.' Below this is a form with three input fields: 'User Name:', 'New Password:', and 'Confirmed Password:'. A red box highlights these three fields. To the right of the form, red text says 'Please input the new user name, password here'. At the bottom of the form are two buttons: 'Apply Change' and 'Reset'.

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.5.2 Firmware Upgrade

The firmware on this wireless router can be easily upgraded. You can check the website (<http://www.cnet.com.tw>) to see if there is any later version of firmware

Notes: Do not power off the device while the firmware is being upgraded

Firmware Upgrade

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

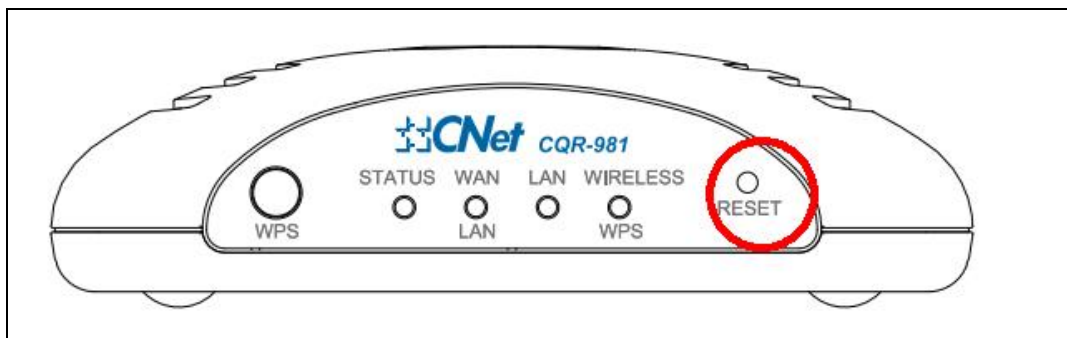
Select File:

Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Caution: The firmware upgrade will not remove your previous settings.

***Reset button:**

On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



4.5.3 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

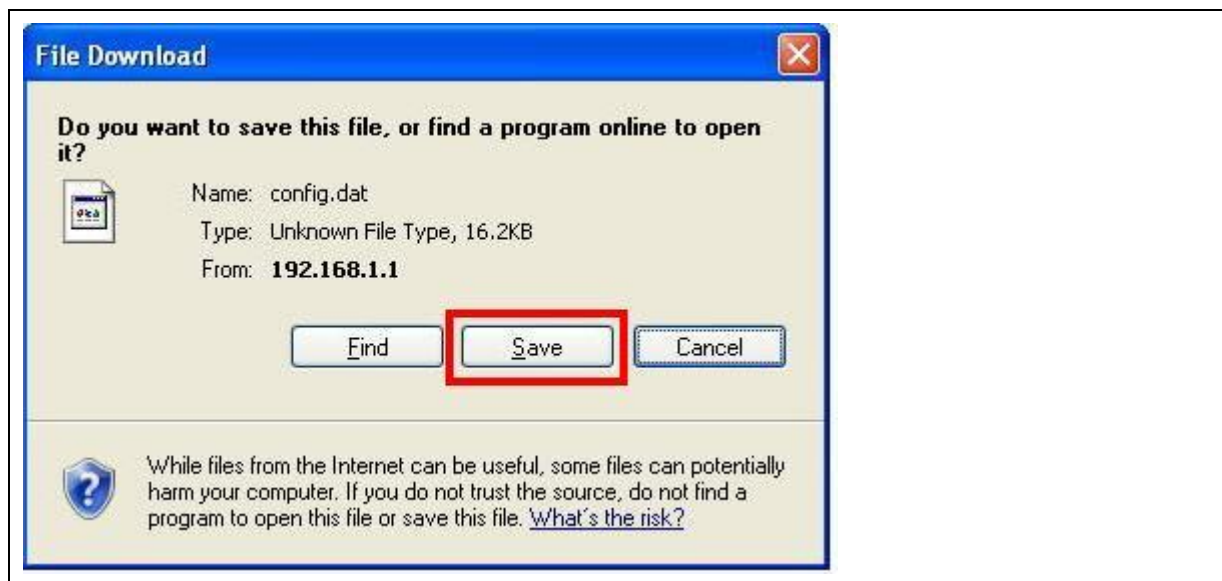
The screenshot shows a web interface titled "Save/Reload Settings". Below the title is a descriptive paragraph: "This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default." There are three main sections: "Save Settings to File:" with a "Save..." button; "Load Settings from File:" with a text input field, a "Browse..." button, and an "Upload" button; and "Reset Settings to Default:" with a "Reset" button. Red boxes and text annotations highlight the "Save..." button with the text "Save to computer", the "Upload" button with the text "Upload the file from PC to router", and the "Reset" button with the text "Reset to default."

a. Save Configuration

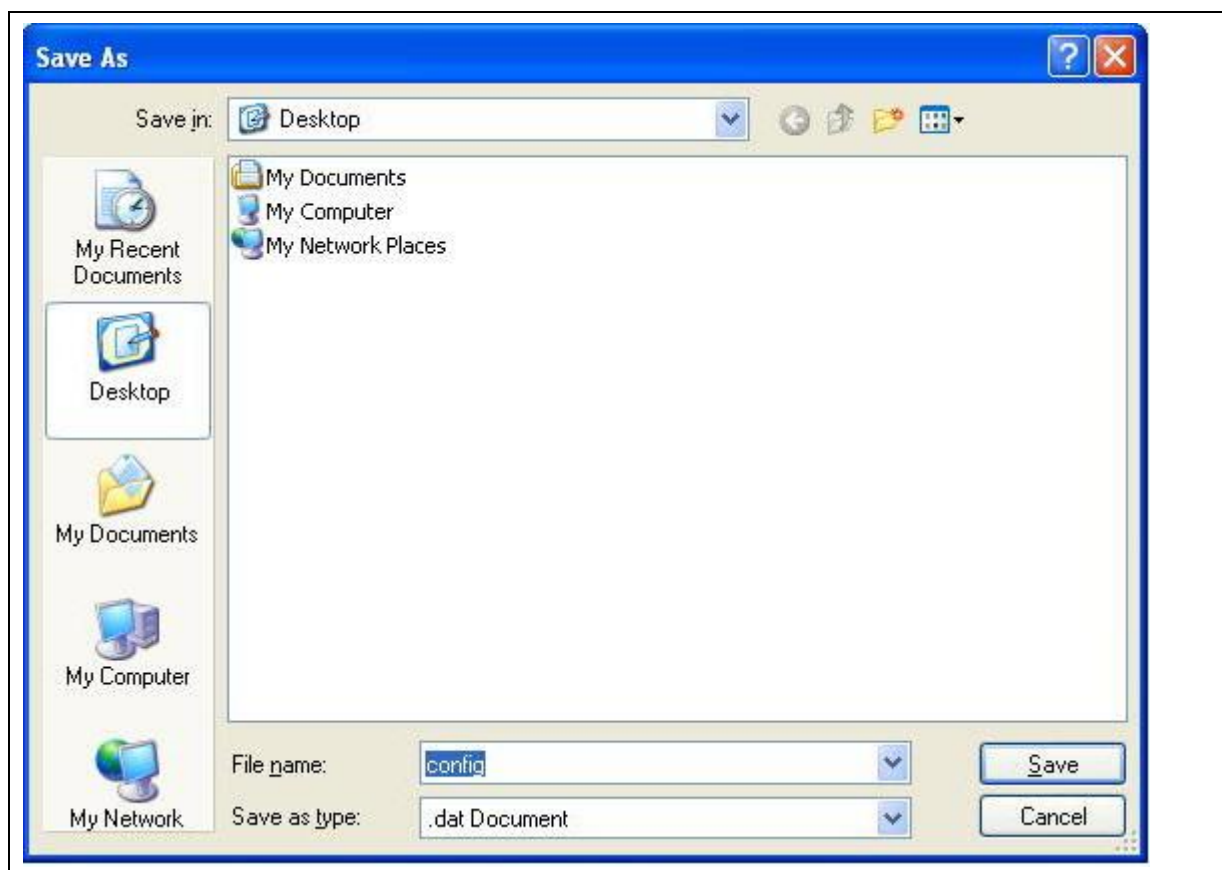
(1) Click **Save**

This screenshot is identical to the one above, showing the "Save/Reload Settings" interface. In this version, only the "Save..." button under the "Save Settings to File:" section is highlighted with a red box.

(2) Please click "Save" to save the configuration to your computer.



(3) Select the location which you want to save file, then click **Save**.



b. Load configuration file

(1) Click **Browser**

Save/Reload Settings

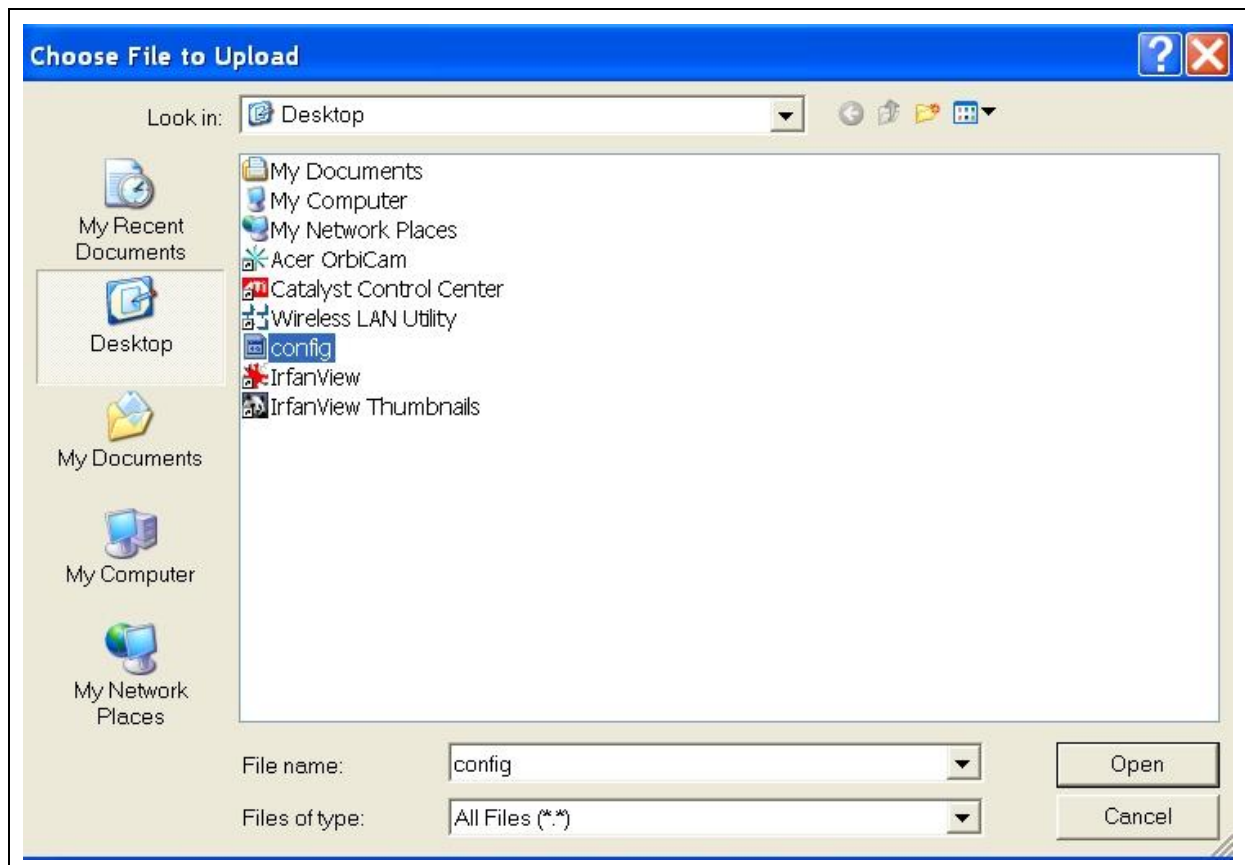
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(2) Select configuration file then click **Open**



(3) Click **Upload** to upload configuration file to CQR-981.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(4) After 90 seconds, CQR-981 will reboot automatically.

(C) Reload factory default setting

1. Please click **Reset**

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.


Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(2) Please click **OK** to start reload factory default setting to CQR-981.

Message from webpage

 Do you really want to reset the current settings to default?

(3) After 90 seconds, CQR-981 will reboot automatically.


4.5.4 Time Zone Setting

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.


Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :  Please select the time zone

☒ Enable NTP client update
☐ Automatically Adjust Daylight Saving

NTP server : ☒ 
☐ (Manual IP Setting)

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable Automatically Adjust Daylight Saving or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data. Or you may click on Refresh to update the system time on the screen.

4.5.5 UPnP Setting

Universal Plug and Play (UPnP) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. CQR-981 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My Network Places**. Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

UPnP Setting

In this page,you can turn on or turn off the UPNP feature of your router.

Enable/Disable UPNP: ☒ Enabled ☐ Disabled

*Enable/Disable UPnP

Select to enable or disable this function.

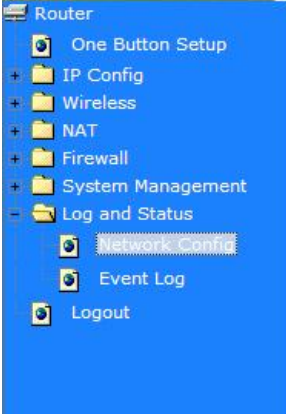
4.6 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



4.6.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP ...information from this page.



A screenshot of the router configuration menu, similar to the one above, but with 'Network Config' selected and highlighted with a dotted border.

Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:3h:5m:57s
Firmware Version	Ver1.0.2
WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CQR-981

4.6.2 Event Log

You could enable the event log feature here.

Router

- One Button Setup
- IP Config
- Wireless
- NAT
- Firewall
- System Management
- Log and Status
 - Network Config
 - Event Log**
 - Logout

System Log

This page can be used to set remote log server and show the system log.

☐ **Enable Log** → **Please select to enable log function.**

☐ system all ☐ wireless ☐ DoS

☐ Enable Remote Log Log Server IP Address:

Item	Description
Enable Log	You may choose to enable Event Log or not
System all, Wireless, DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply & Cancel	Click on Apply button to add the settings into the list table. Click on Cancel button to clean the setting on this page.

*The following figure is an example when users click **Apply Changes** to record the event log.

☒ **Enable Log**

☒ **system all**
☐ **wireless**
☐ **DoS**

☐ **Enable Remote Log**

Log Server IP Address:

Apply Changes

Comtrack

Oday 00:00:17 PPTP netfilter connection tracking: registered
Oday 00:00:17 PPTP netfilter NAT helper: registered
Oday 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
Oday 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
Oday 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
Oday 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
Oday 00:00:17 Freeing unused kernel memory: 64k freed
Oday 00:00:17 mount /proc file system ok!
Oday 00:00:17 mount /var file system ok!
Oday 00:00:17 device eth0 entered promiscuous mode
Oday 00:00:17 device wlan0 entered promiscuous mode
Oday 00:00:17 TPT: unreasonable target TSSI 0
Oday 00:00:17 br0: port 2(wlan0) entering listening state
Oday 00:00:17 br0: port 1(eth0) entering listening state
Oday 00:00:17 br0: port 2(wlan0) entering listening state

Refresh

Clear

4.7 Logout

This function logs out the user.

Router

One Button Setup

IP Config

Wireless

NAT

Firewall

System Management

Log and Status

Logout

Logout

This page is used to logout.

Do you want to logout ?

Apply Change

Chapter 5 AP Mode Advanced Configuration

5.1 IP Config

In this category, you can setup the IP rules under AP Mode.

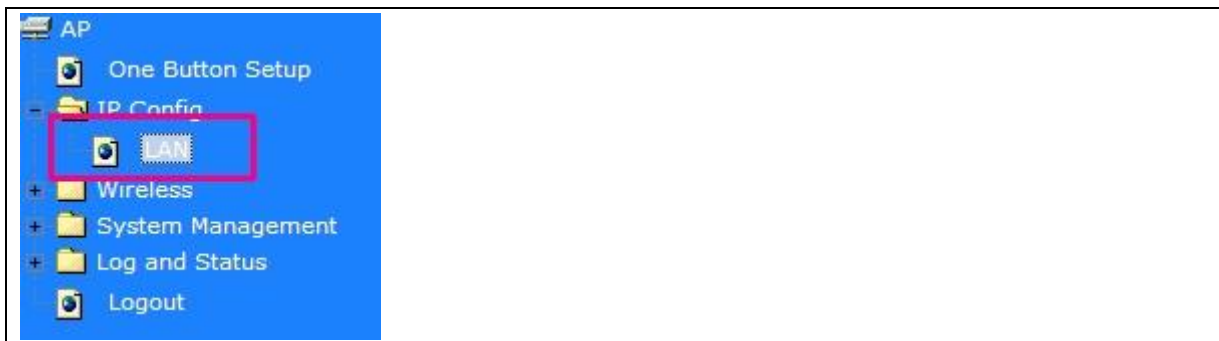
Default IP Address: 192.168.1.254

Default IP subnet mask: 255.255.255.0

WEB login User Name: admin

WEB login Password: admin

5.1.1 LAN Setup



Please click on **LAN** of **IP Config** and follow the below setting.

5.1.2 LAN Interface Setup

This page is used to configure for local area network which connects to the LAN port of your Access Point. Here users may change the setting for IP address, Subnet Mask, DHCP, etc.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="button" value="Client"/> <input type="button" value="v"/>
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
Static DHCP:	<input type="button" value="Set Static DHCP"/>
Device Name:	<input type="text" value="CQR-980"/>
802.1d Spanning Tree:	<input type="button" value="Disabled"/> <input type="button" value="v"/>
Clone MAC Address:	<input type="text" value="000000000000"/>

Item	Description
IP Address	The default IP address is 192.168.1.254
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Please enter the Default Gateway address for LAN interface.
DHCP	Click to select Disabled , Client or Server in different operation mode of LAN access point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range
Static DHCP	Configures how static DHCP address are assigned to client (only available when DHCP server is enabled)
Device Name	Configures the device name of the router.
802.1d Spanning Tree	IEEE 802.1d Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN, This function is optional.
Clone MAC Address	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

5.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Security**, **Access Control**, **WDS settings**, and **WPS**. Please read below for the setting instruction.



5.2.1 Wireless Basic Settings

The Wireless Basic Settings include Band, Mode, SSID, Channel Number and other wireless settings.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:

2.4 GHz (B+G+N) ▼

Mode:

AP ▼

Multiple AP

Network Type:

Infrastructure ▼

SSID:

CNet

Channel Width:

40MHz ▼

Control Sideband:

Upper ▼

Channel Number:

11 ▼

Broadcast SSID:

Enabled ▼

WMM:

Enabled ▼

Data Rate:

Auto ▼

Associated Clients:

Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☒ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

ESSID_Cnet

Apply Change

Reset

Item	Description
Disable Wireless LAN Interface	Turn off the wireless service.
Band	Please select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	Please select the mode. It has 3 modes to select:(AP, Client, WDS, AP+WDS). Multiple APs provides users another 4 different SSID for connection. Users can add or limit the properties for each connection. Please check Section 5.2.1.1
SSID	Service Set identifier, the default SSID is CNet , users can define to any.
Channel Width	Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.
Channel Number	Please select the channel; it has Auto, 1, 2~11 or 13 options.
Broadband SSID	User may choose to enable Broadcast SSID or not.
Data Rate	Please select the data transmission rate.
Associate Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

5.2.1.1 Multiple APs

Multiple APs provides users another 4 different SSIDs for connection. Each SSID could be set with different data rate, WMM and access type.

Multiple APs

This page shows and updates the wireless setting for multiple APs.

No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_1	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show
AP2	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_2	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show
AP3	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_3	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show
AP4	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N) ▾	MultipleAP_4	Auto ▾	Enabled ▾	Enabled ▾	LAN+WAN ▾	Show

Item	Description
Enable	Enable or disable the service.
Band	Select the frequency.
SSID	Enter the SSID.
Data Rate	Select the data transmission rate.
Access	Enable this function can let clients use two access types: a. LAN+WAN: the client can access to the Internet and access in the router's GUI. b. WAN: the client can only access to the Internet.
Active Client List	Display the properties of the client which is connecting successfully.
Apply Changes	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

5.2.2 Wireless Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Preamble Type: ☒ Long Preamble ☐ Short Preamble

IAPP: ☒ Enabled ☐ Disabled

Protection: ☐ Enabled ☒ Disabled

Aggregation: ☒ Enabled ☐ Disabled

Short GI: ☒ Enabled ☐ Disabled

WLAN Partition: ☐ Enabled ☒ Disabled

RF Output Power: ☒ 100% ☐ 70% ☐ 50% ☐ 35% ☐ 15%

Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.

Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and 15%.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

5.2.3 Wireless Security Setup

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link.** There are five Encryption types supported: "None", "WEP", "WPA (TKIP)", "WPA2(AES)", and "WPA2 Mixed".

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

802.1x Authentication: ☐

1. Encryption -- WEP Key

1.1 Set WEP Key: This section provides 64bit and 128bit WEP encryptions and two different shared key formats (ASCII and Hex) for wireless network.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

802.1x Authentication: ☐

Authentication: ☐ Open System ☐ Shared Key ☒ Auto

Key Length:

Key Format:

Encryption Key:

802.1x Authentication: It is a safety system by using authentication to protect your wireless network.

4. Encryption – WPA (WPA, WPA2, and WPA2 Mixed), WPA Authentication Mode
- Enterprise (RADIUS): Please fill in the RADIUS server Port, IP Address, and Password

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode:

☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite:

☐ TKIP ☐ AES

Pre-Shared Key Format:

Pre-Shared Key:

- Personal (Pre-Shared Key): Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode:

☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite:

☐ TKIP ☐ AES

WPA2 Cipher Suite:

☐ TKIP ☒ AES

Pre-Shared Key Format:

Pre-Shared Key:

5. Apply Change & Reset: Click on '**Apply Changes**' to save setting data. Or click '**Reset**' to reset all the input data.

5.2.4 Wireless Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on “**Apply Changes**” to save the new addition. To delete a MAC address, select its corresponding checkbox under the **Select** column and click on “**Delete Selected**” button.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

MAC Address: Comment:

Apply Changes Reset

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected Delete All Reset

Take the wireless card as the example.

- (1) Here is the example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then fill in the MAC address what you plan to block in the MAC Address field. Click **Apply Changes** to save the setting.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Deny Listed

MAC Address: Comment:

Apply Change Reset

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected Delete All Reset

(2) The MAC address what you set will be displayed on the **Current Access Control List**.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Deny Listed

MAC Address: Comment:

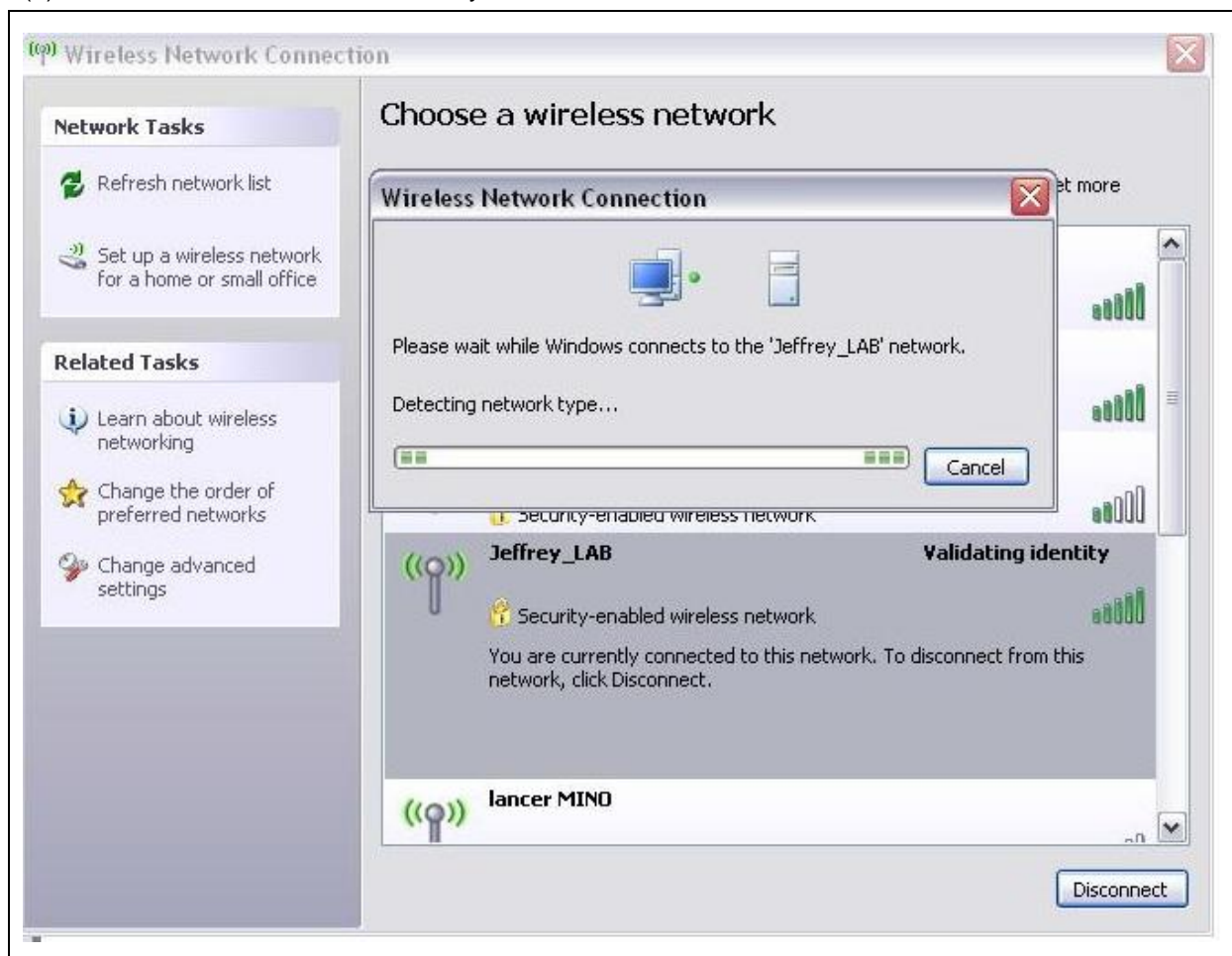
Apply Change Reset

Current Access Control List:

MAC Address	Comment	Select
00:18:f8:63:8a:54		<input type="checkbox"/>

Delete Selected Delete All Reset

(3) The wireless client will be denied by the wireless router.



5.2.5 WDS Settings

When selected in the Basic Settings page and enabled here, Wireless Distribution System (WDS) enables the router to be used as a wireless bridge. Two Wireless-G Routers in bridge mode can communicate with each other through their wireless interfaces. To accomplish this, all wireless routers should be set to the same channel and the MAC address of other AP / Routers should be entered in the table.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☐ **Enable WDS**

MAC Address:

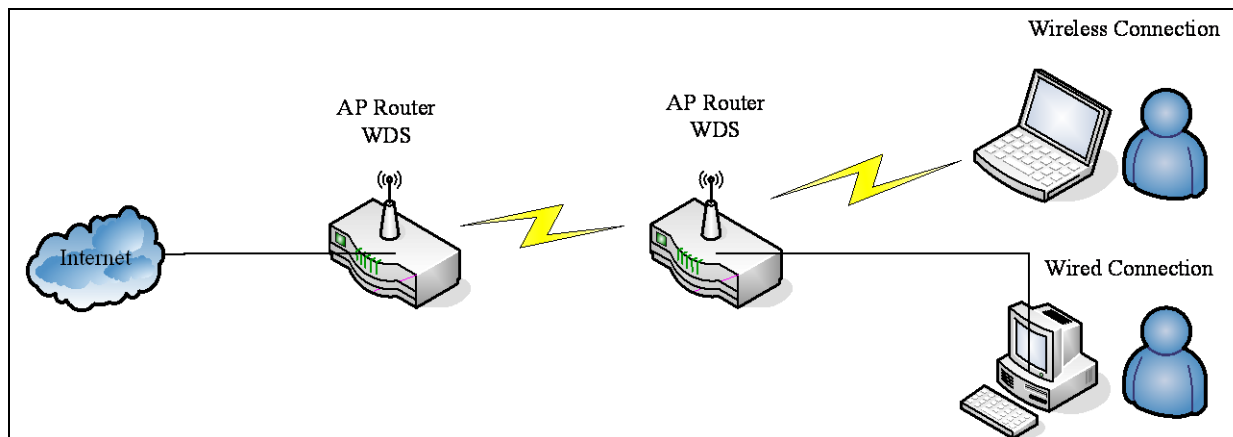
Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

The WDS explanation as the following picture.



*Please follow the below instructions to setup the WDS connection.

(1) Please check the MAC address and Channel number from the upper lever device.

Network Config	
This page shows the current status and some basic settings of the device.	
System	
Uptime	1day:3h:2m:45s
Firmware Version	Ver1.0.1
WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CNet
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:96:b1
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:b1

(2) Set the connection mode to “AP+WDS” from “Wireless Basic Setting”, and then select the channel number(in this example is “11”). Click **Apply Changes** to save the setting.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N) ▼

Mode: AP+WDS ▼

Multiple AP

Network Type: Infrastructure ▼

SSID: CNet

Channel Width: 40MHz ▼

Control Sideband: Upper ▼

Channel Number: 11 ▼

Broadcast SSID: Enabled ▼

WMM: Enabled ▼

Data Rate: Auto ▼

Associated Clients: Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface: ESSID_Cnet

Apply Change

Reset

- (3) Enable WDS function from the page – “WDS Setting”, and then fill in the upper level device MAC address. Click **Apply Changes** to save the setting data.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☒ Enable WDS

MAC Address: 000e68ff05c8

Data Rate: Auto ▼

Comment:

Apply Changes

Reset

Set Security

Show Statistics

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

Delete Selected

Delete All

Reset

(4) The WDS AP List will show the WDS device MAC address after reboot.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☒ **Enable WDS**

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:0e:68:ff:05:c8	Auto		<input type="checkbox"/>

(5) Set "Broadcast SSID" to disable from page "Wireless Basic Setting".

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

Band:

Mode:

Network Type:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Broadcast SSID:

WMM:

Data Rate:

Associated Clients:

☐ **Enable Mac Clone (Single Ethernet Client)**

☐ **Enable Universal Repeater Mode (Acting as AP and client simultaneously)**

SSID of Extended Interface:

(6) Go to the upper level device WDS setting page and fill in the MAC address

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☒ **Enable WDS**

MAC Address:

000e68ff05do

Data Rate:

Auto

Comment:

Please input the MAC address of this router.

Apply Changes

Reset

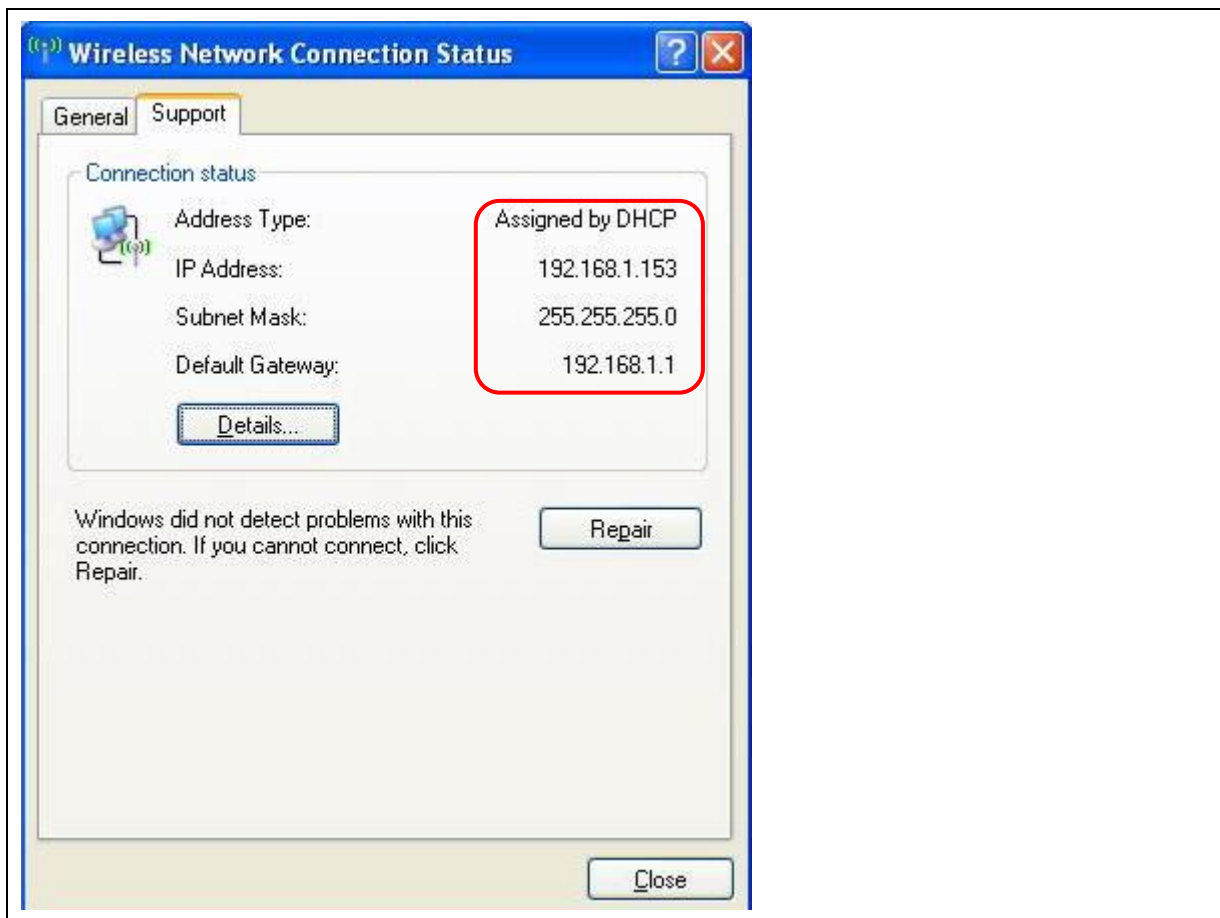
Set Security

Show Statistics

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
<div><div>Delete Selected</div><div>Delete All</div><div>Reset</div></div>			

(7) You will receive an IP address from the upper lever device.



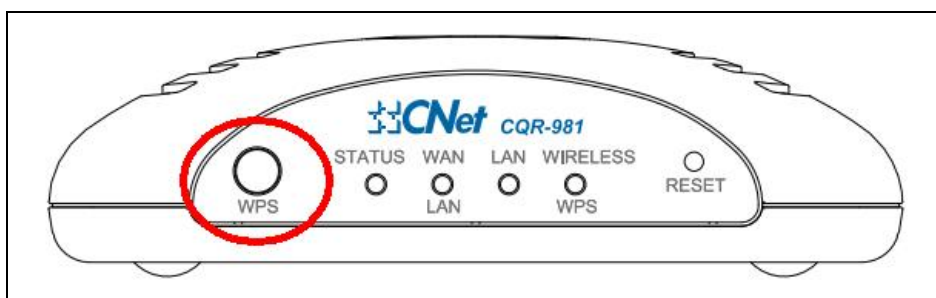
5.2.6 WPS

This page allows user to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronize it's setting and connect to the Access Point in a minute without any hassle. CQR-981 could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.

PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

Please find the WPS button from the following illustrate



When users select a specific model on wireless base station, the clients can connect to the base by selecting the same model.

The connection procedures of PIN and PBC are almost the same. The small difference between those two is:

Users input the PIN of wireless card in the base station first; it will limit the range of the clients. It is faster to establish a connection on PIN model.

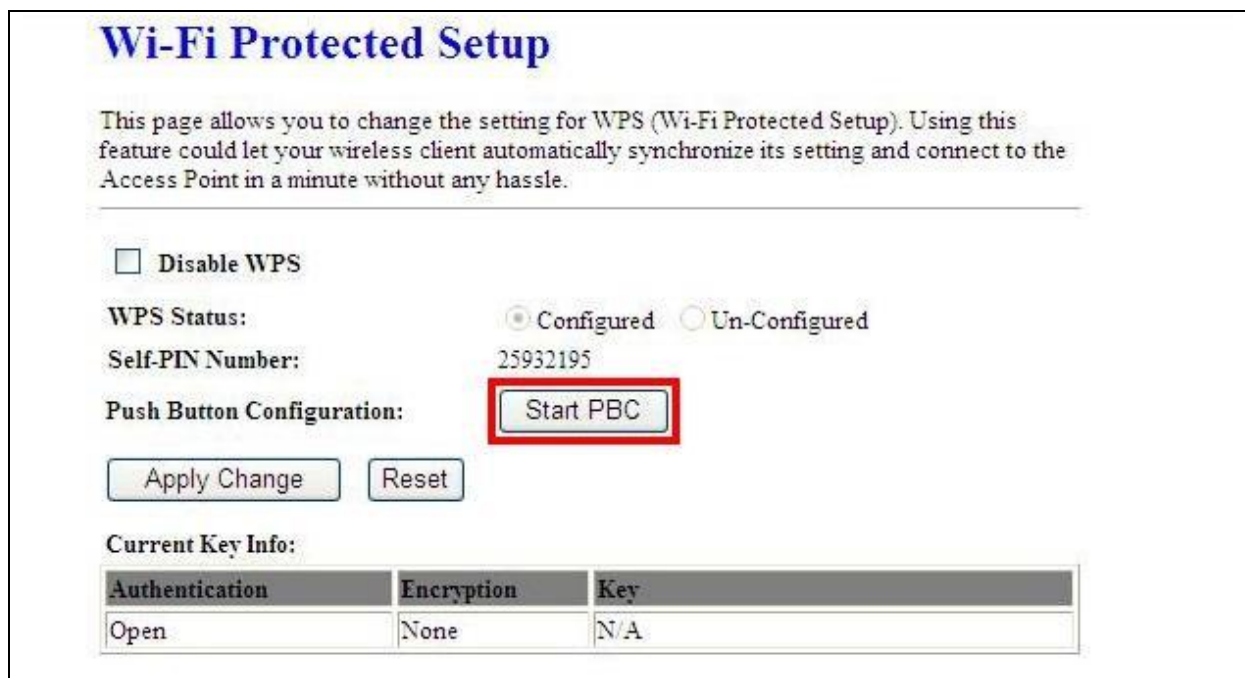
On PBC model, users push the WPS button to activate the function, and then the wireless client must push the WPS button in 2 mins to enter the network. The client will search to see if there is any wireless base station which supports WPS is activating. If the client finds a matching base, the connection will be established. The speed of establishing a connection is slower than the PIN model because of this extra step.

On the other hand, users need to input the information of the wireless card into the register interface. It might lead to the failure of connection, if users make mistakes on inputting. On PBC model, users only need to click the WPS button on both sides to make a connection. It is easier to operate.

This page supports **Start PBC** and **Start PIN**; please read the following instructions

* Start PBC:

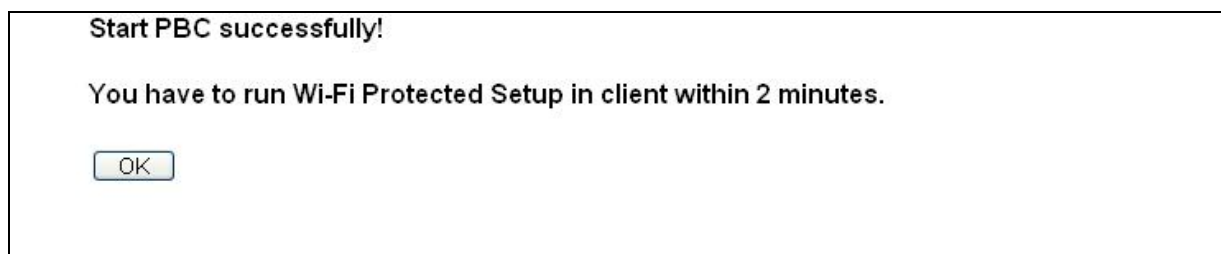
(1) Click **Start PBC** to connect to the wireless network card.



The image shows a web interface titled "Wi-Fi Protected Setup". It contains a checkbox for "Disable WPS", "WPS Status" with radio buttons for "Configured" (selected) and "Un-Configured", a "Self-PIN Number" field with the value "25932195", and a "Push Button Configuration" section with a "Start PBC" button highlighted by a red rectangle. Below these are "Apply Change" and "Reset" buttons. At the bottom, there is a "Current Key Info" section with a table showing authentication, encryption, and key details.

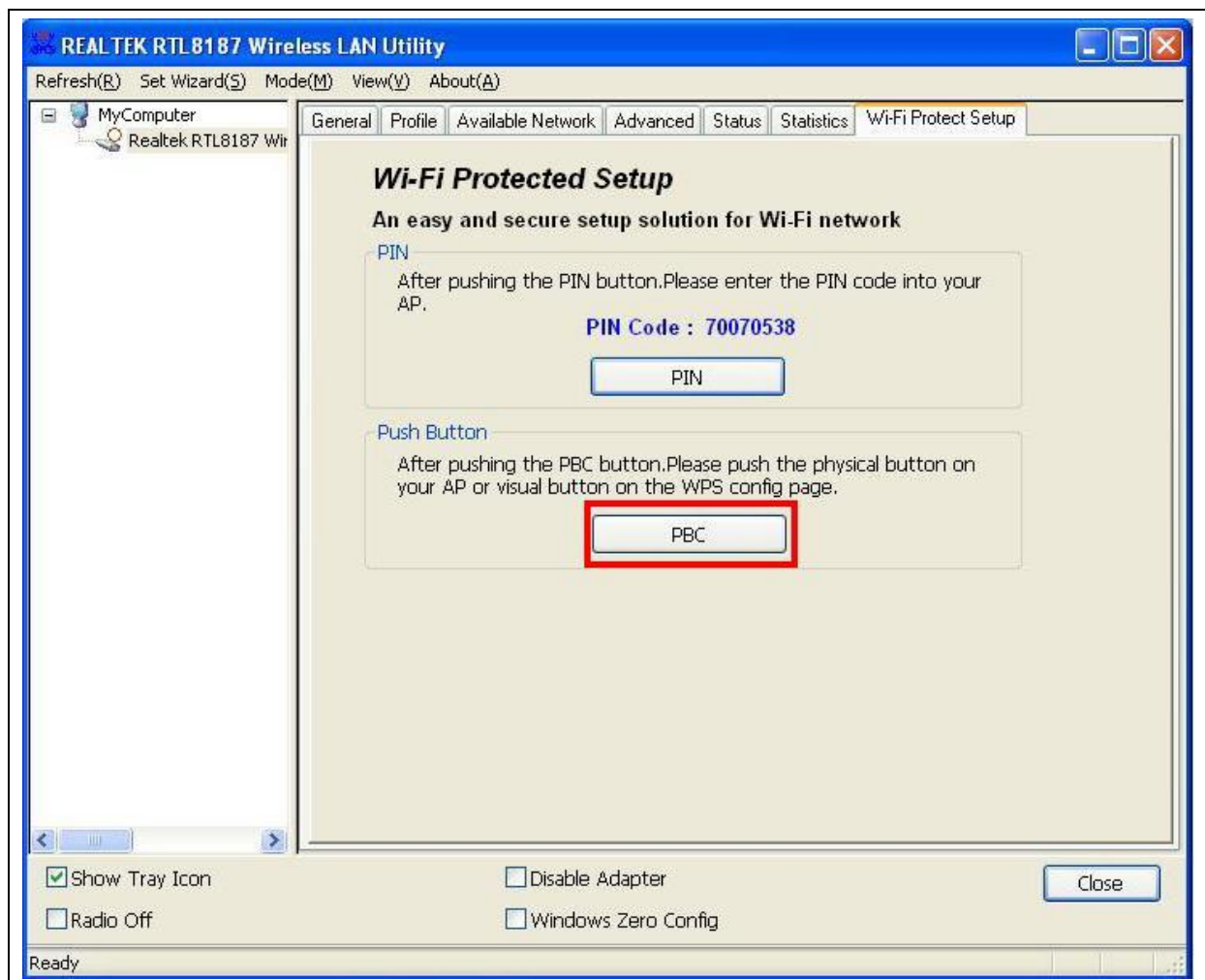
Authentication	Encryption	Key
Open	None	N/A

(2) Click **OK** to start WPS process.

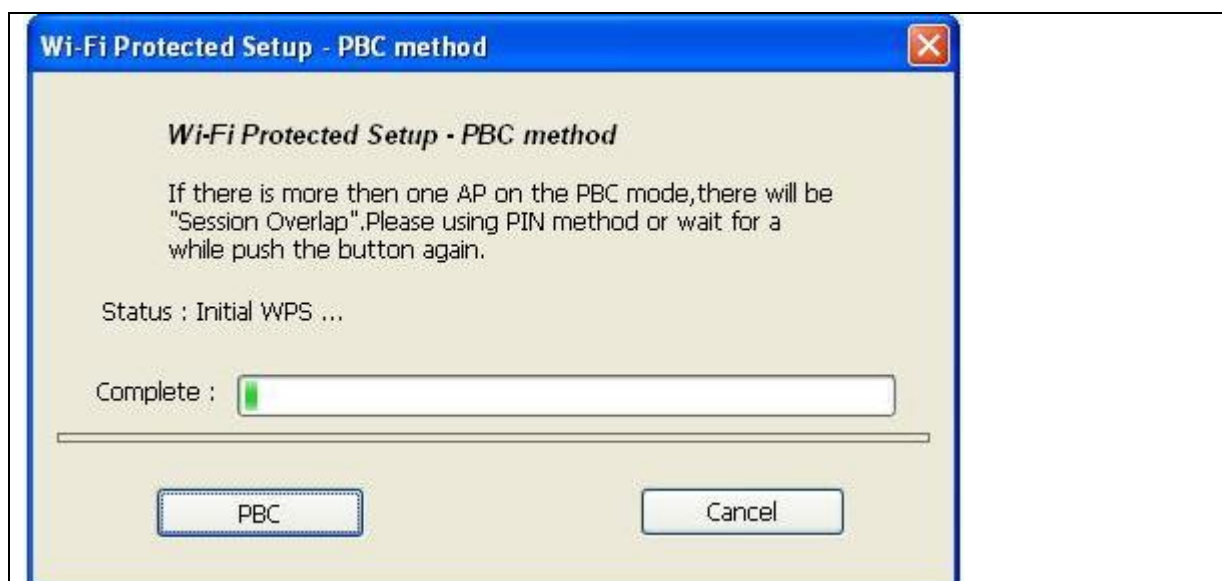


The image shows a success message dialog box. It contains the text "Start PBC successfully!" and "You have to run Wi-Fi Protected Setup in client within 2 minutes." Below the text is an "OK" button.

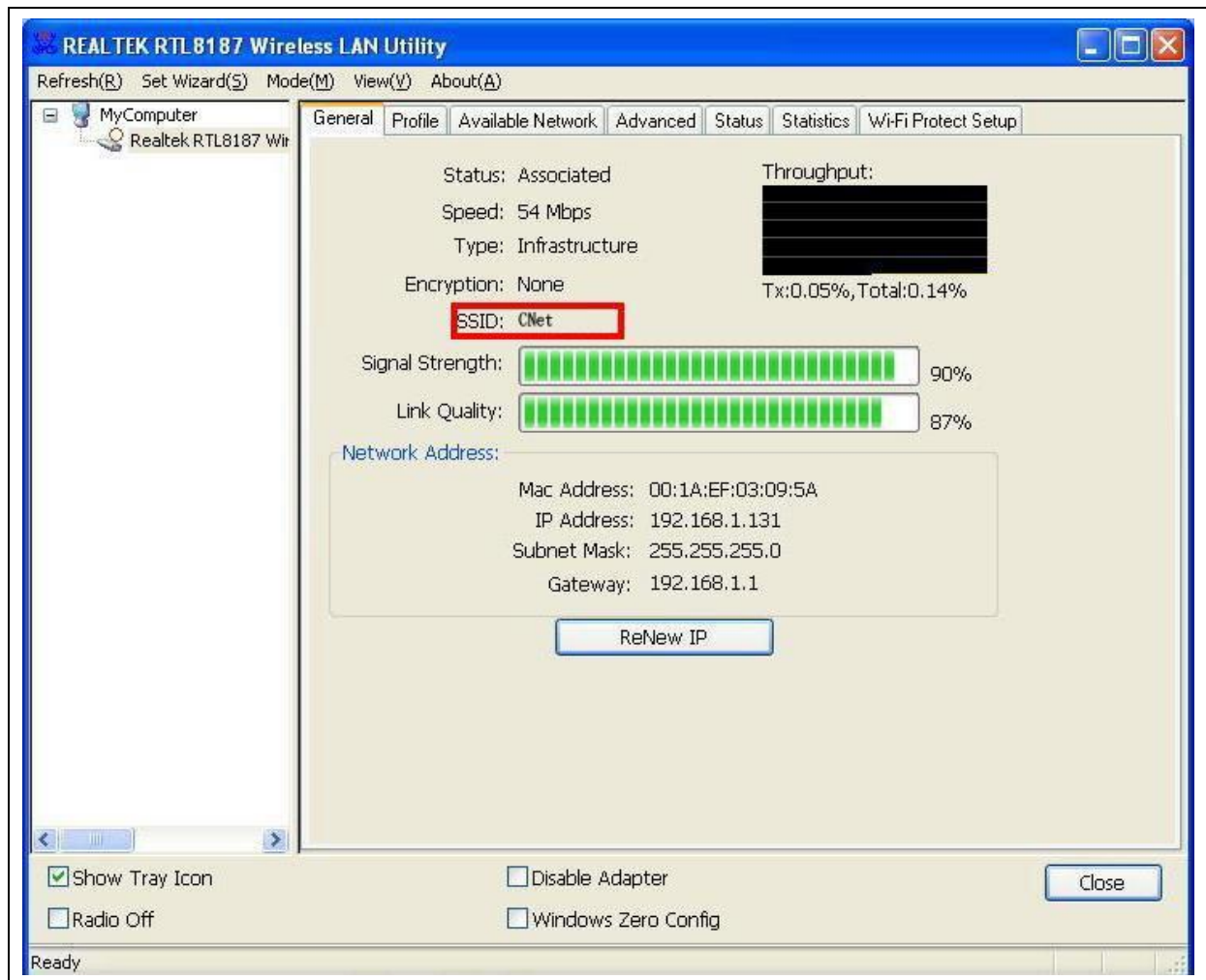
(3) Open the configuration page of the wireless card. Click the **Wi-Fi Protect Setup**, and then click **PBC** to start the WPS process.



(4) The WPS is being processed.

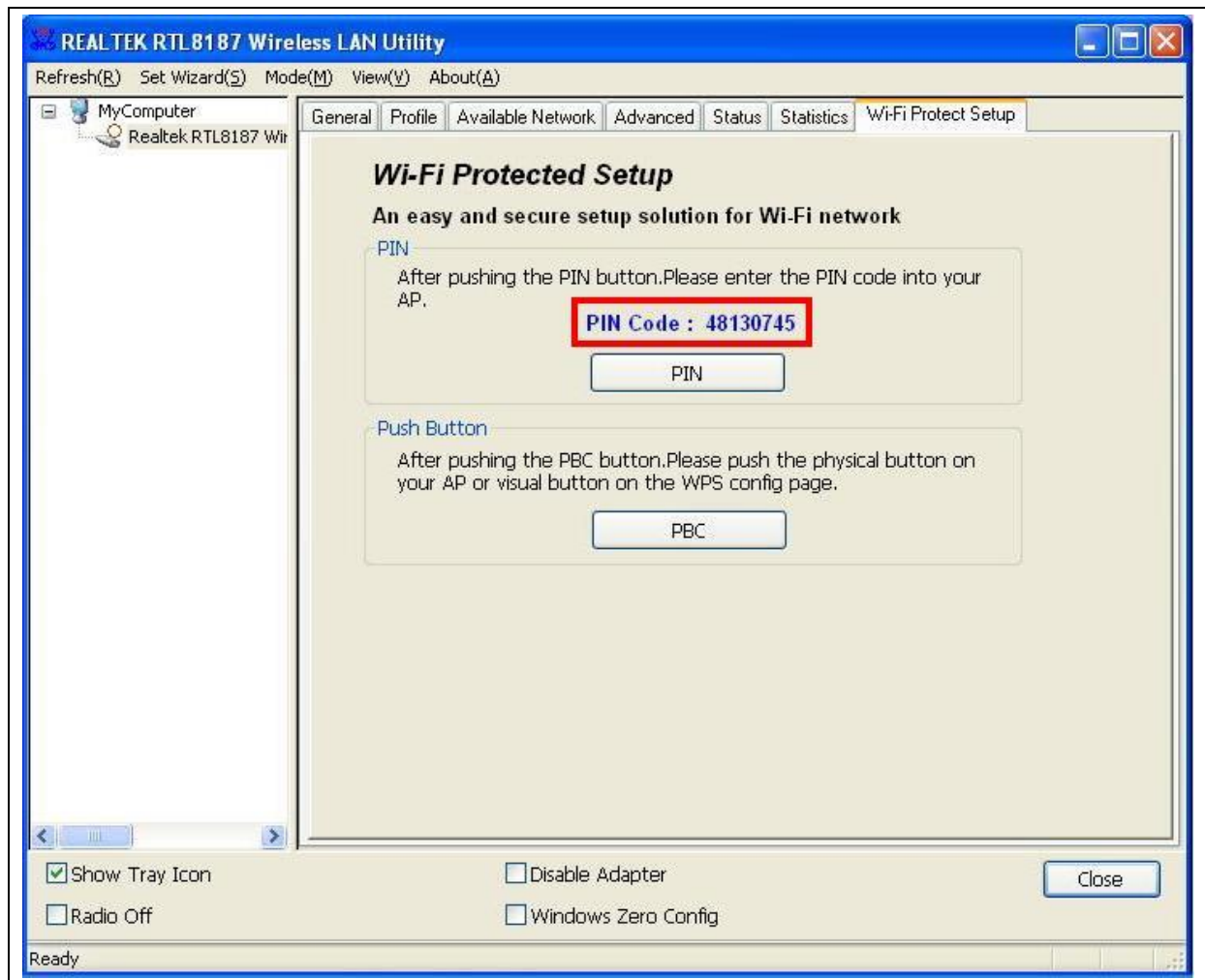


- (5) The USB dongle will receive the connection information from wireless router if the dongle has connected to the wireless router successfully.

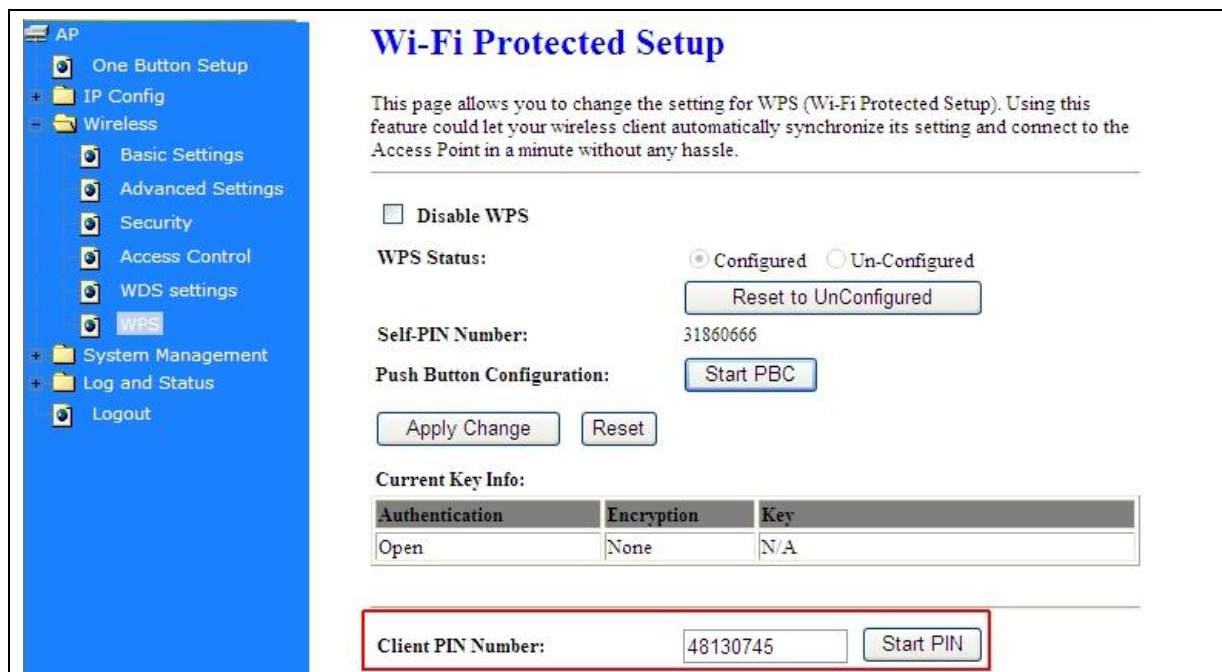


* Start PIN:

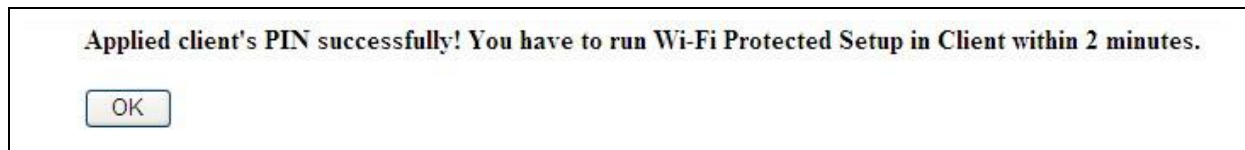
- (1.) Get the WPS PIN number from wireless card and write it down.



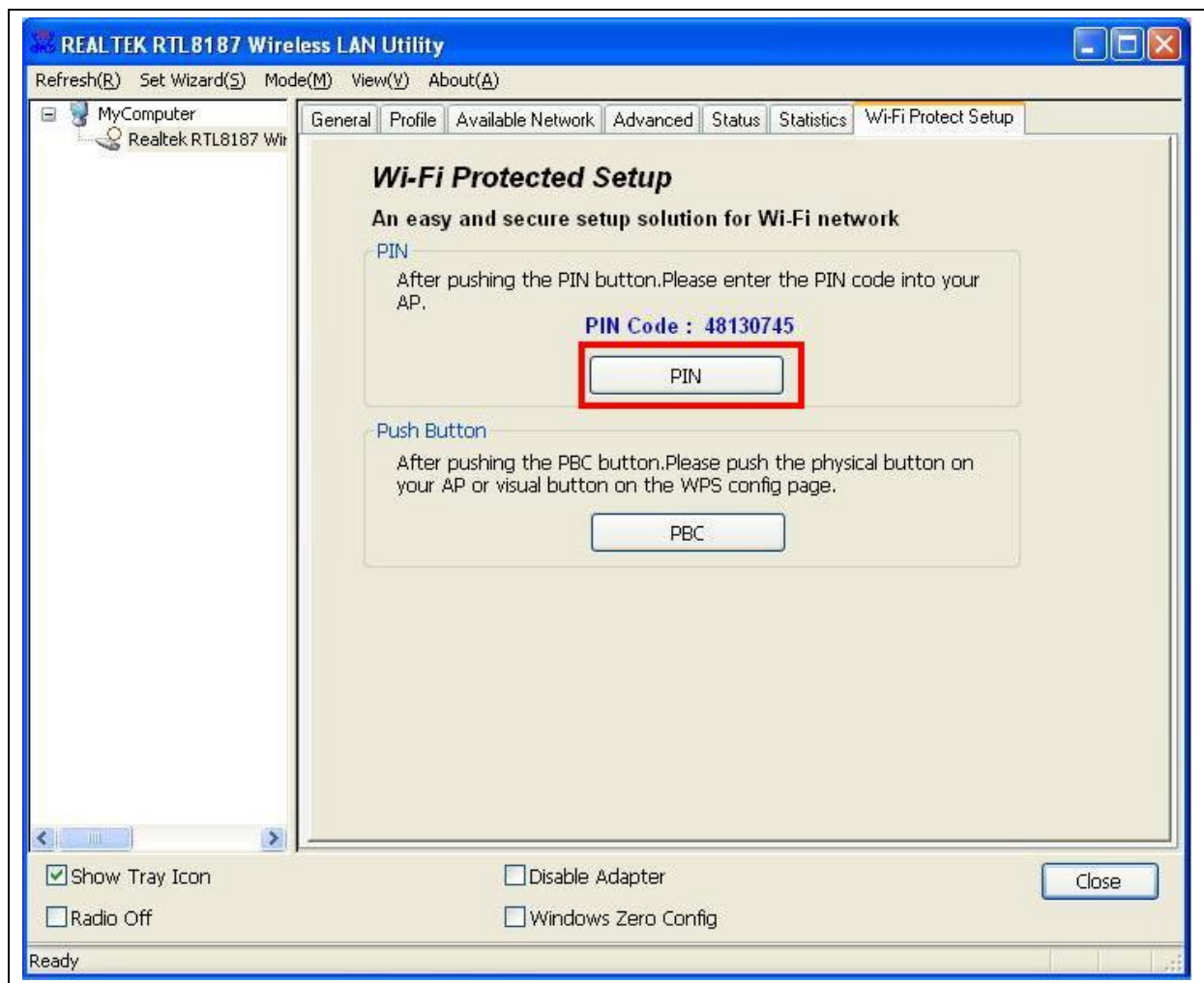
(2) Fill in the PIN number from the wireless card in Client PIN Number field, and then click "Start PIN".



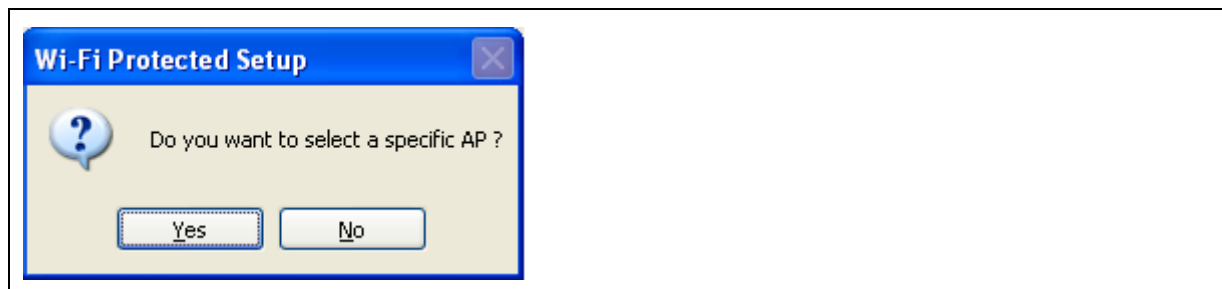
(3) Click **OK** to starts process.



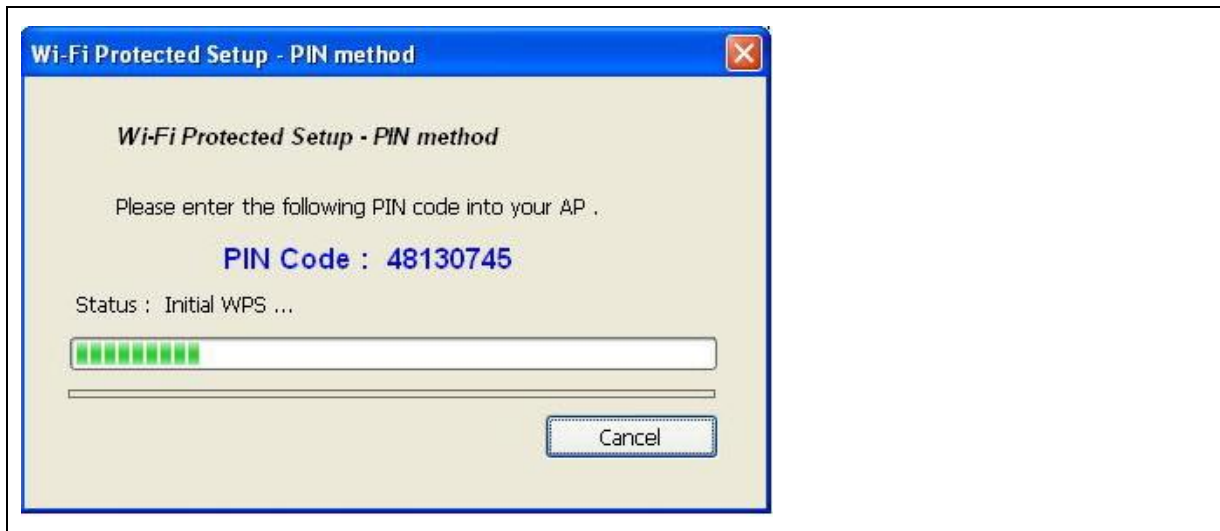
(4) Click **PIN** to start the WPS process with the wireless router.



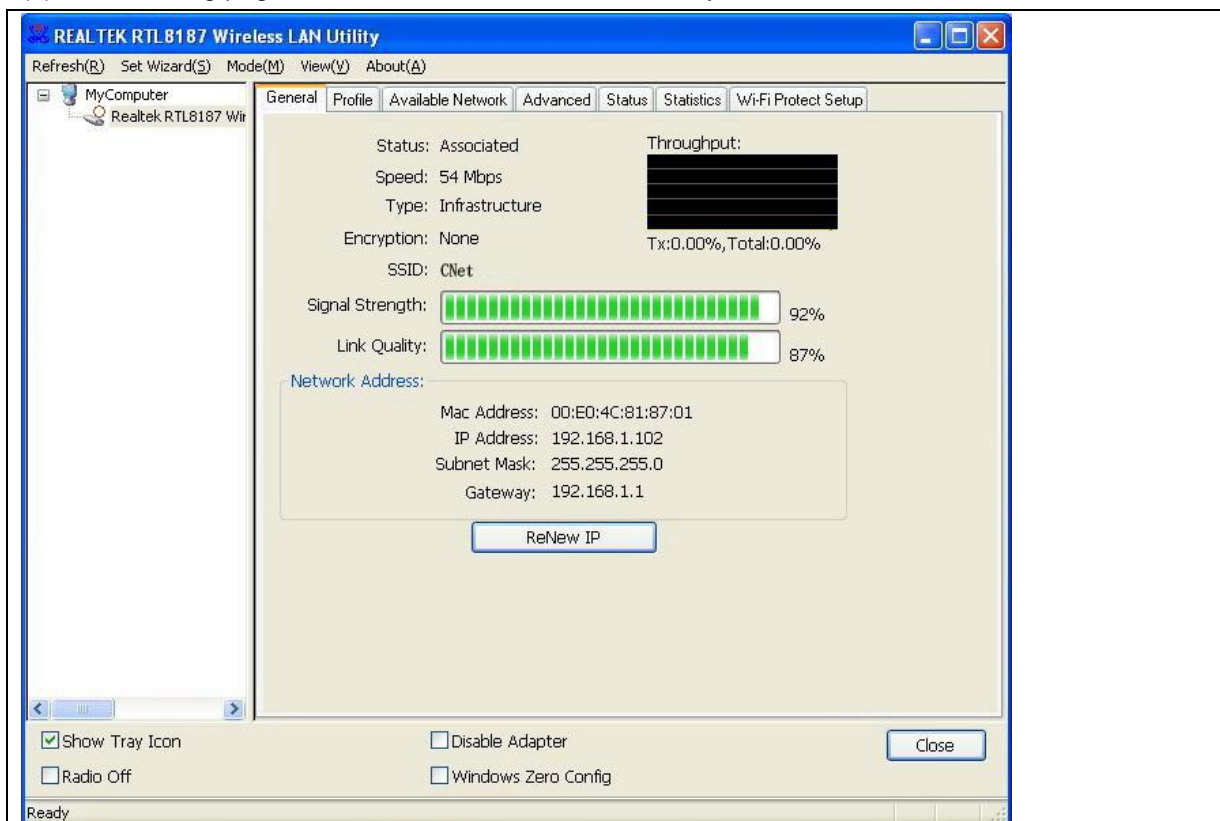
(5) Click **No**, then USB Dongle will select AP automatically.



(6) WPS is in processing.

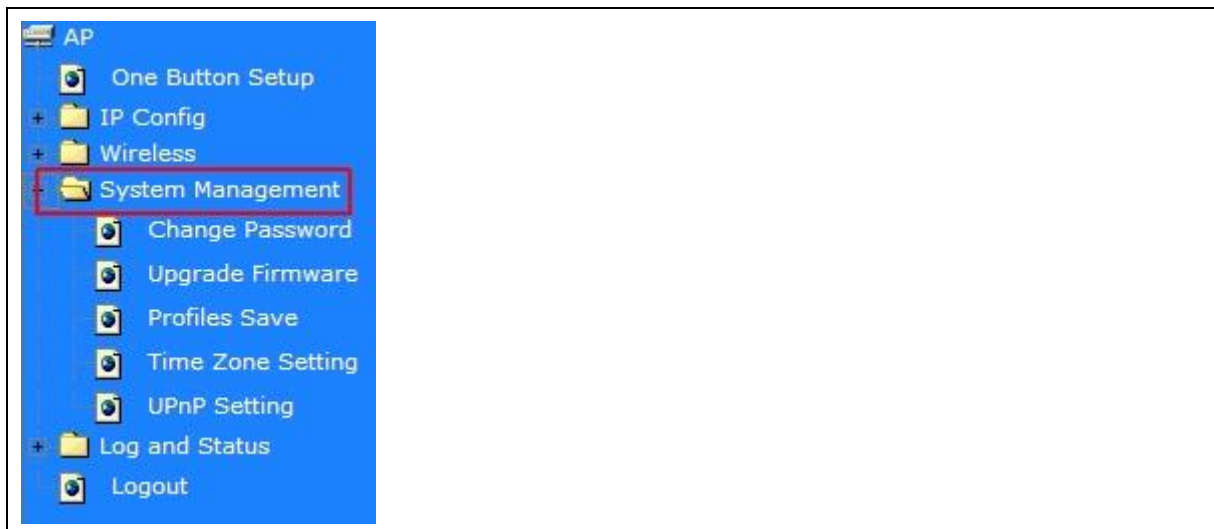


(7) The following page shows the wireless card has already connected to the wireless router.



5.3 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.



5.3.1 Change Password

Users can set or change user name and password used for accessing the web management interface in this section.

A screenshot of the 'Change Password' page in a web interface. The page has a blue sidebar on the left with a menu containing 'One Button Setup', 'IP Config', 'Wireless', 'System Management' (expanded), 'Change Password' (highlighted with a red box), 'Upgrade Firmware', 'Profiles Save', 'Time Zone Setting', 'UPnP Setting', 'Log and Status', and 'Logout'. The main content area has a title 'Change Password' in blue. Below the title is a warning message: 'This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.' There are three input fields: 'User Name:', 'New Password:', and 'Confirmed Password:'. A red box highlights these fields. To the right of the fields, red text says 'Please input the new user name, password here'. At the bottom, there are two buttons: 'Apply Change' and 'Reset'.

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.3.2 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website (<http://www.cnet.com.tw>) to see if there is any later version of

firmware. Download the firmware to your computer, click **Browser** and point to the new firmware file. Click **Upload** to upgrade the firmware. You can't make any move unless the machine reboot completely.

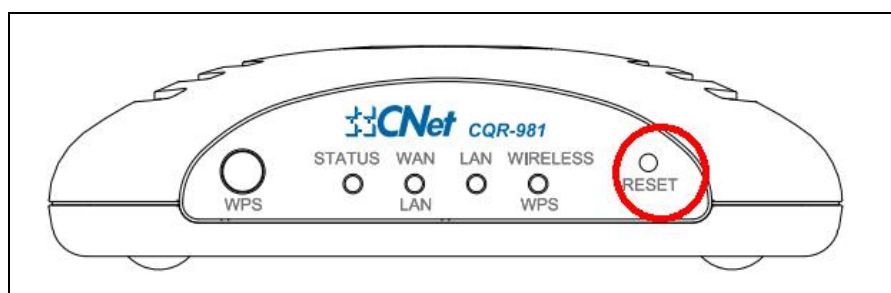


Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Caution: The firmware upgrade will not remove your previous settings.

* Reset button:

On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 10 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



5.3.1 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Save...

Save to computer

Load Settings from File:

Browse...

Upload

Upload the file from PC to router

Reset Settings to Default:

Reset

Reset to default.

a. Save Configuration

(1) Click **Save**

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Save...

Load Settings from File:

Browse...

Upload

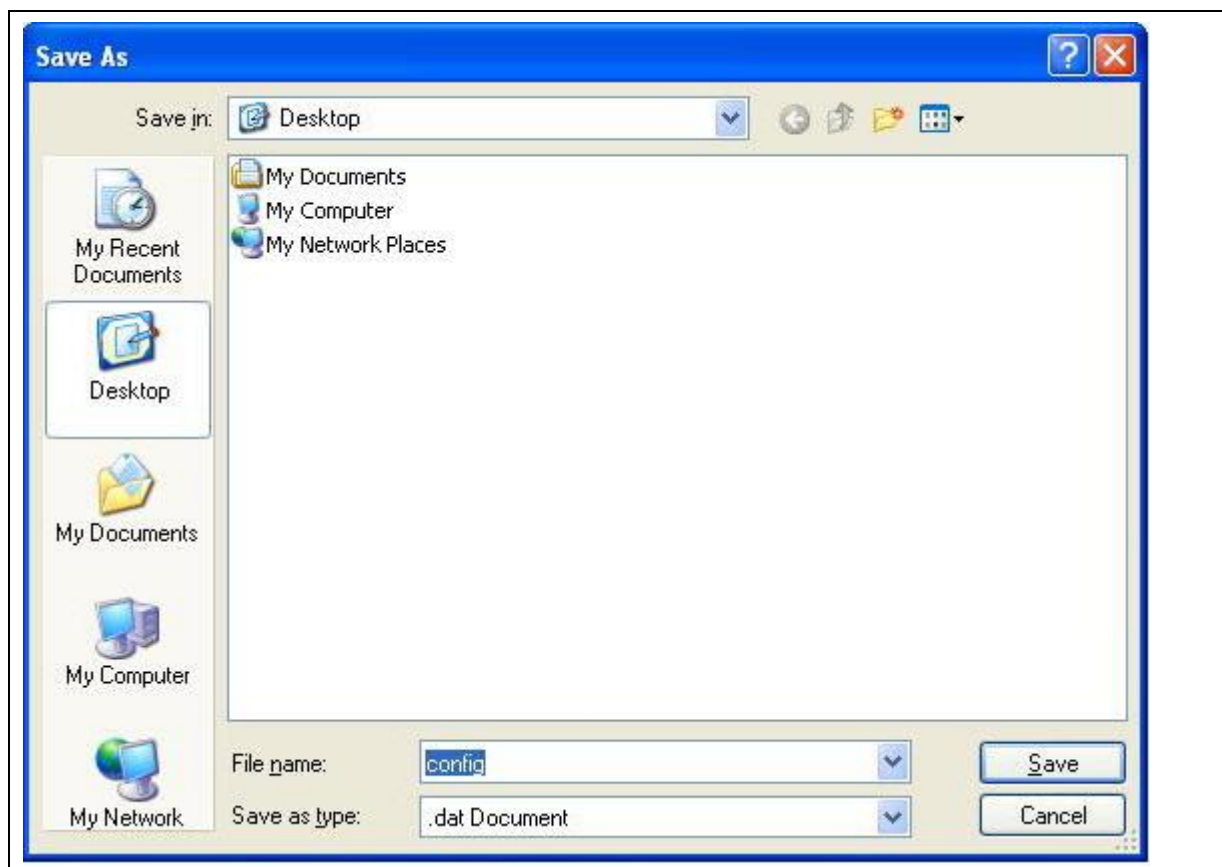
Reset Settings to Default:

Reset

(2) Please click “**Save**” to save the configuration to your computer.



(3) Select the location which you want to save file, then click **Save**.



b. Load configuration file

(1) Click **Browser**

Save/Reload Settings

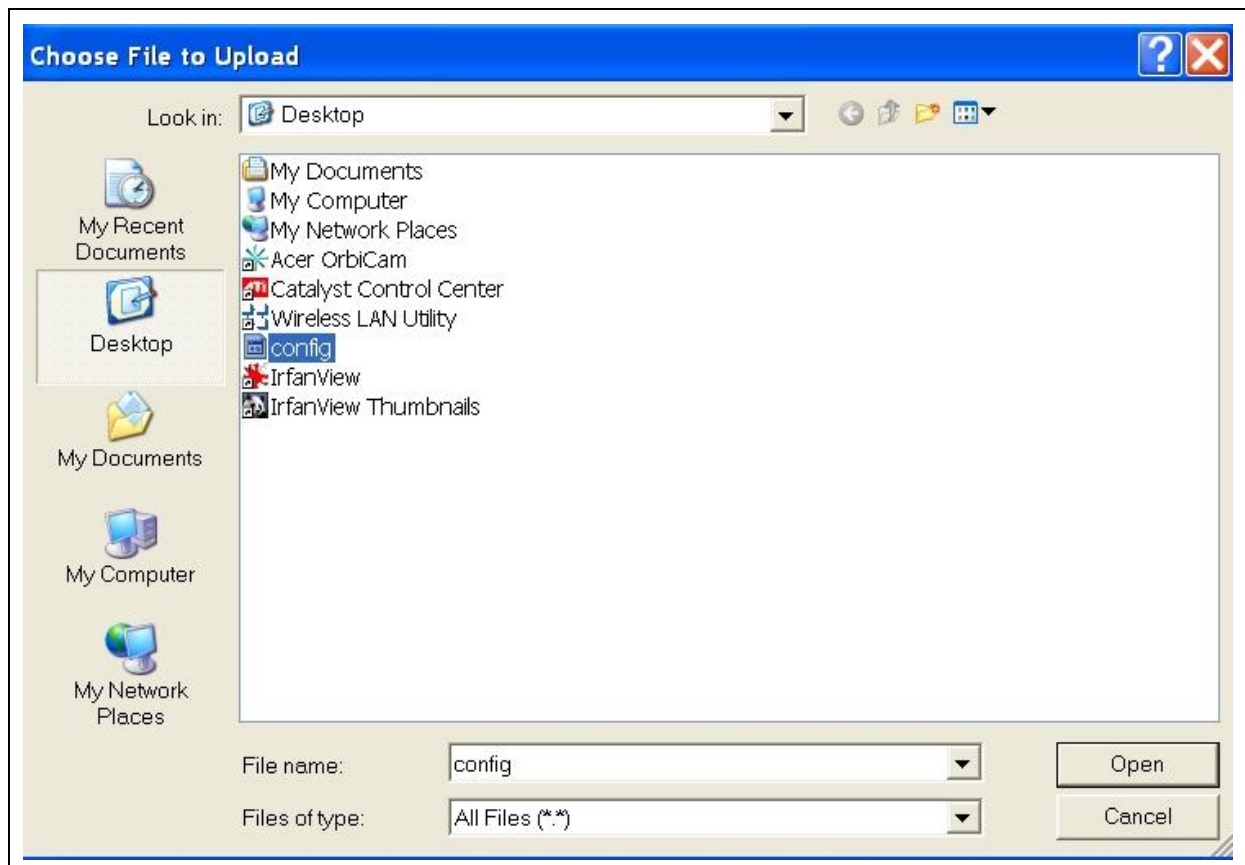
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(2) Select configuration file then click **Open**



(3) Click **Upload** to upload configuration file to CQR-981.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Save...

Load Settings from File:

ministrator\Desktop\config.dat

Browse...

Upload

Reset Settings to Default:

Reset

(4) After 90 seconds, CQR-981 will reboot automatically.

(C) Reload factory default setting

1. Please click **Reset**

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Save...

Load Settings from File:

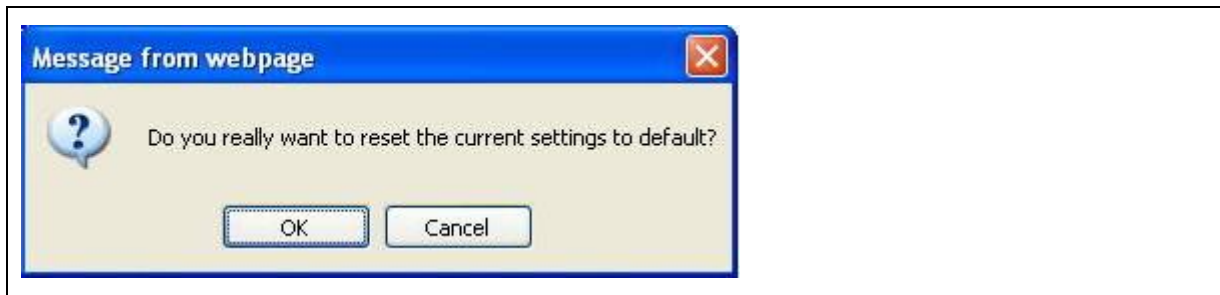
Browse...

Upload

Reset Settings to Default:

Reset

(2) Please click **OK** to start reload factory default setting to CQR-981.



(3) After 90 seconds, CQR-981 will reboot automatically.


5.3.2 Time Zone Setting

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.


Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :  Please select the time zone

☒ Enable NTP client update
☐ Automatically Adjust Daylight Saving

NTP server : ☒ 
☐ (Manual IP Setting)

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable Automatically Adjust Daylight Saving or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data. Or you may click on Refresh to update the system time on the screen.

5.3.3 UPnP Setting

Universal Plug and Play (UPnP) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. CQR-981 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My Network Places**. Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

UPnP Setting

In this page,you can turn on or turn off the UPNP feature of your router.

Enable/Disable UPNP: ☒ Enabled ☐ Disabled

*Enable/Disable UPnP

Select to enable or disable this function.

5.3.4 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



5.3.5 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP ...information.

A screenshot of the 'Network Config' page in the AP configuration interface. The left sidebar is the same as in the previous image, but 'Network Config' is now highlighted with a red rectangle. The main content area has a white background and a blue header 'Network Config'. Below the header is a subtitle: 'This page shows the current status and some basic settings of the device.' Below this is a horizontal line. The settings are organized into sections: 'System' (blue header), 'WirelessConfiguration' (blue header), and 'LAN Configuration' (blue header). Each section contains a table of settings.

System	
Uptime	0day:4h:34m:8s
Firmware Version	Ver1.0.2

WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CQR-981
Channel Number	6
Encryption	Disabled
MAC Address	00:08:a1:c7:a5:2b
Associated Clients	0

LAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Client
MAC Address	00:08:a1:c7:a5:2b

5.3.6 Event Log

You may enable the event log feature here.

AP

- One Button Setup
- IP Config
- Wireless
- System Management
- Log and Status
 - Network Config
 - Event Log**
 - Logout

☐ **Enable Log**
☐ system all ☐ wireless ☐ DoS
☐ **Enable Remote Log** Log Server IP Address:

→ **Please select to enable log function.**

Item	Description
Enable Log	You may choose to enable Event Log or not.
System all, Wireless, & DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply Changes & Refresh & Clear	Click on Apply Changes to save the setting data. Click on Refresh to renew the system time, or on Clear to clear all the record.

* The following figure is an example when users click **Apply Changes** to record the event log.

☒ **system all** ☐ wireless ☐ DoS
☐ **Enable Remote Log** Log Server IP Address:

```

Jan 1 00:00:39 sr 0:0:0:1: Attached scsi generic sg1 type 5
Jan 1 00:00:39 usb-storage: device scan complete
Jan 1 00:00:39 FAT: utf8 is not a recommended IO charset for FAT
filesystems, filesystem will be case sensitive!
Jan 1 00:00:39 =====stp port dev mapping reinit=====
Jan 1 00:00:39 mapping: lan phycisal [port0] <====>pseudo [port0]
Jan 1 00:00:39 mapping: lan phycisal [port1] <====>pseudo [port1]
Jan 1 00:00:39 mapping: lan phycisal [port2] <====>pseudo [port2]
Jan 1 00:00:39 mapping: lan phycisal [port3] <====>pseudo [port3]
Jan 1 00:00:39 mapping: lan phycisal [port4] <====>pseudo [port4]
Jan 1 00:00:39 mapping table is 0 1 2 3 4
Jan 1 00:00:39
Jan 1 00:00:39 RTL STP disabled
Jan 1 00:00:39 RTL865x Port 0 state=DISABLED*****1
Jan 1 00:00:39 device eth0 entered promiscuous mode
  
```

5.4 Logout

This function logs out the user.



Chapter 6 Advanced Configuration for Wi-Fi AP Mode

6.1 IP Config

In this category, you can setup the IP rules under WiFi-AP Mode.

Default IP Address: 192.168.1.254

Default IP subnet mask: 255.255.255.0

WEB login User Name: admin

WEB login Password: admin

6.1.1 IP Config -- LAN



6.1.2 LAN Interface Setup

This page is used to configure for local area network which connects to the LAN port of your Access Point. Here users may change the setting for IP address, Subnet Mask, DHCP, etc.

WIFI AP

One Button Setup

IP Config

LAN

Wireless

System Management

Log and Status

Logout

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:

192.168.1.254

Subnet Mask:

255.255.255.0

Default Gateway:

0.0.0.0

DHCP:

Client

DHCP Client Range:

192.168.1.100

-

192.168.1.200

Show Client

Static DHCP:

Set Static DHCP

Device Name:

CQR-980

802.1d Spanning Tree:

Disabled

Clone MAC Address:

000000000000

Apply Change

Reset

Item	Description
IP Address	The default IP address is 192.168.1.254
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Please enter the Default Gateway address for LAN interface.
DHCP	Click to select Disabled , Client or Server in different operation mode of LAN access point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range
Static DHCP	Configures how static DHCP address are assigned to client (only available when DHCP server is enabled)
Device Name	Configures the device name of the router.
802.1d Spanning Tree	IEEE 802.1d Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN, This function is optional.
Clone MAC Address	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Apply Change & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Site Survey**, **Security**, **Access Control**, and **WPS**. Please read below for the setting instructions.



6.2.1 Wireless Basic Setting

The basic settings related to the wireless are specified as following.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N) ▼

Mode: Client ▼ Multiple AP

Network Type: Infrastructure ▼

SSID: CQR-981

Channel Width: 40MHz ▼

Control Sideband: Upper ▼

Channel Number: 6 ▼

Broadcast SSID: Enabled ▼

WMM: Enabled ▼

Data Rate: Auto ▼

Associated Clients: Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☒ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface: ESSID_CQR-981

Apply Change

Reset

Item	Description
Disable Wireless LAN Interface	Turn off the wireless function.
Band	Please select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	In Wi-Fi AP mode only support Clint mode
Network Type	Please select the network type, it has 2 options: Infrastructure or Ad hoc .
SSID	Service Set identifier, the default SSID is CQR-981 , users can define to any.
Channel Width	Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.

Broadcast SSID	User may choose to enable Broadcast SSID or not.
Data Rate	Please select the data transmission rate.
Associated Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
Enable Universal Repeater Mode (Action as AP and Client simultaneously)	Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (Please check Note 1).
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

Note.

1. Enable Universal Repeater Mode (Acting as AP and Client simultaneously)

Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.)

Ex: When users enable the Universal Repeater to connect to the upper level device, please input the channel and SSID of the upper level device on router's GUI. Click on **Apply Changes** to save the settings. (The DHCP in IP config needs to be disabled.)

Users can go to the network Config section and check the information of upper level in Wireless Repeater Interface Configuration.

WIFI AP

One Button Setup

IP Config

Wireless

System Management

Log and Status

Network Config

Event Log

Logout

Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:8m:54s
Firmware Version	Ver1.0.2
WirelessConfiguration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	CQR-981
Channel Number	4
Encryption	Disabled
MAC Address	00:00:00:00:00:00
State	Scanning
WirelessRepeater Interface Configuration	
Mode	AP
ESSID	ESSID_CQR-981
Encryption	Disabled
MAC Address	00:00:00:00:00:00
Associated Clients	0
LAN Configuration	

Caution: when users enable the wireless encryption. The upper level and lower devices can connect to each other even if their encryption types are not the same.

6.2.2 Wireless Advanced Settings

Please complete the wireless advanced settings as following instructions.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Preamble Type: ☒ Long Preamble ☐ Short Preamble

IAPP: ☒ Enabled ☐ Disabled

Protection: ☐ Enabled ☒ Disabled

Aggregation: ☒ Enabled ☐ Disabled

Short GI: ☒ Enabled ☐ Disabled

WLAN Partition: ☐ Enabled ☒ Disabled

RF Output Power: ☒ 100% ☐ 70% ☐ 50% ☐ 35% ☐ 15%

Apply Change

Reset

Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346 Bytes.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.
Preamble Type	Preamble is the first subfield of PPDU, which is the appropriate frame format form transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble. The Short Preamble

	option improves throughput performance. Select the suit Preamble as Short or Long Preamble.
IAPP	Inter Access Point Protocol. Allow seamless roaming between Access Points in your wireless network.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust the RF output power to get the best wireless connection. Users can choose from 100%, 70%, 50%, 35%, and 15%.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.2.3 Wireless Site Survey

This function provides users to search existing wireless APs or wireless base stations from ISP. You can connect to a wireless AP manually in Wi-Fi AP mode. The designed AP will appear on SSID column in Wireless Basic Setup page.

Please click on **Refresh** to refresh the list. Click **Connect** after select an existing AP to connect.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when WiFi AP mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal
Encryption: None					

Refresh
Connect

6.2.4 Wireless Security Setup

4 encryption types could be selected here, please follow below instructions for the setting.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

802.1x Authentication: ☐

1. Encryption – WEP

1.1 Set WEP Key

This section provides 64bit and 128bit WEP encryptions for wireless network. Users can also choose ASCII and Hex shared Key format to protect data.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

802.1x Authentication: ☐

Authentication: ☒ Open System ☐ Shared Key ☐ Auto

Key Length:

Key Format:

Encryption Key:

1.2 802.1x Authentication

It is a safety system by using authentication to protect your wireless network.

Please choose between WEP 64bits and WEP 128bits.

2. Encryption – WPA (WPA 、WPA2 & WPA2 Mixed)

WPA Authentication Mode

2.1 Enterprise (RADIUS)

Please input the Port, IP Address, and Password of Authentication RADIUS Server.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite: ☒ TKIP ☐ AES

Pre-Shared Key Format:

Pre-Shared Key:

2.2 Personal (Pre-Shared Key)

Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite: ☒ TKIP ☐ AES

WPA2 Cipher Suite: ☐ TKIP ☒ AES

Pre-Shared Key Format:

Pre-Shared Key:

3. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6.2.5 Wireless Access Control

The function of access control is to allow or deny users to access the router by according MAC address, it is optional. If you select **Allowed Listed**, then only those clients whose MAC address is listed on access control can connect to your base station. If you select **Deny Listed**, those clients whose MAC address is listed on access control can't connect to your base station.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: → Users may enable or disable this function.

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
<div><input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/></div>		

Take the wireless card as the example.

- (1) We will use **Deny Listed** as an example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then input the MAC address of wireless card in MAC Address field. Click **Apply Changes** to save the setting data.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Deny Listed 

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

- (2) You will find out that the MAC address appears on **Current Access Control List**, it means the initiation is completed.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

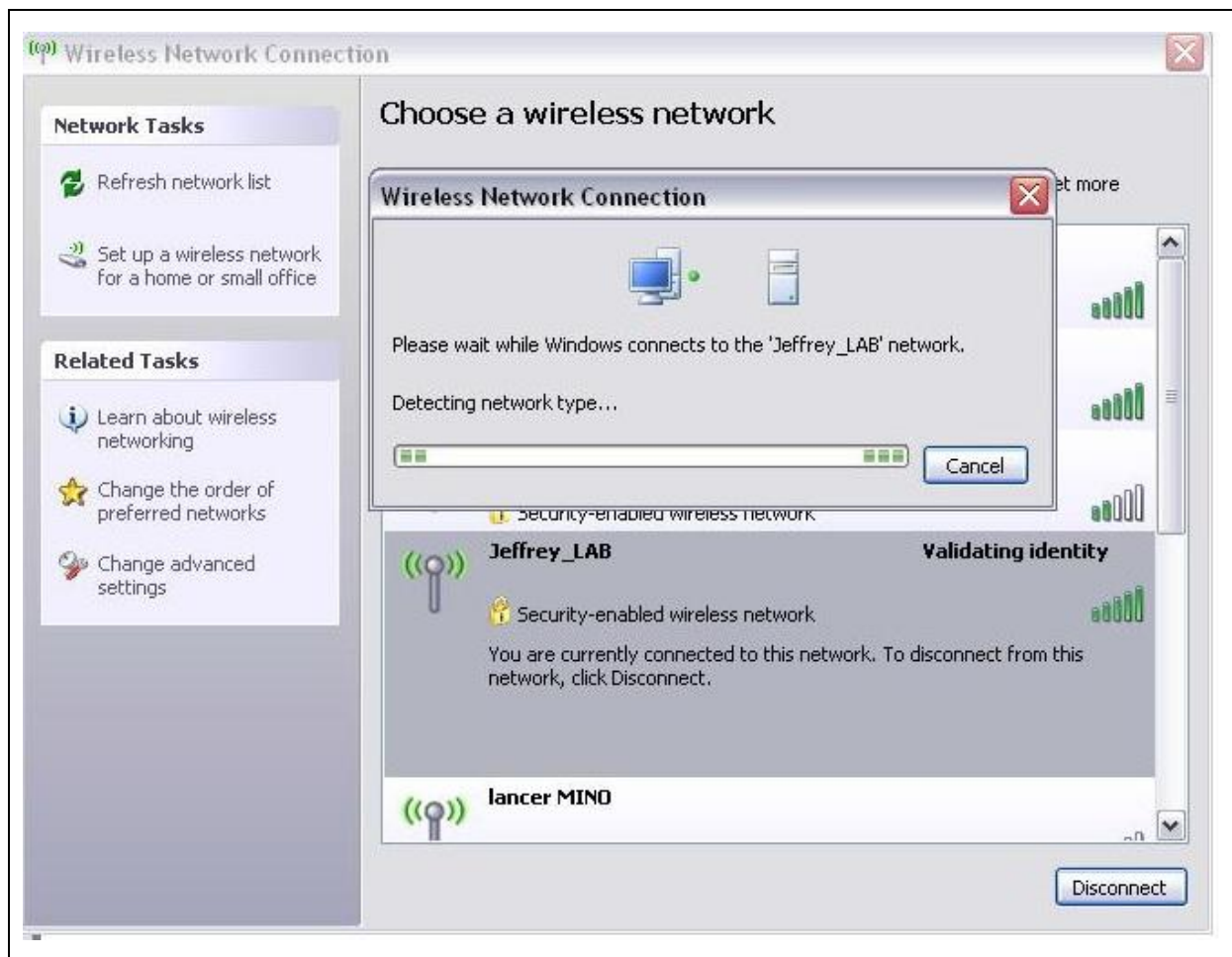
Wireless Access Control Mode: Deny Listed 

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
00:d0:41:b0:d1:17		<input type="checkbox"/>

- (3) Please open wireless card UI and try to connect to this router. You will find out that the connection request will be denied.



6.2.6 WPS Setting

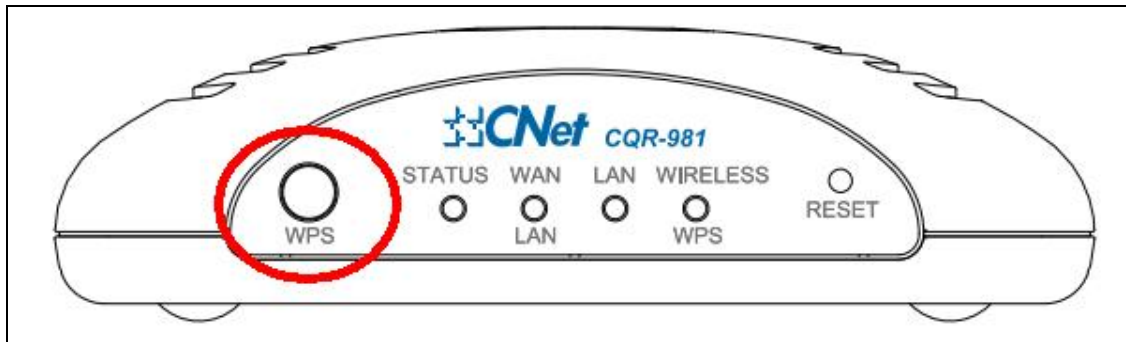
Wi-Fi Protected Setup, it can simplify the procedures of wireless encryption between CQR-981 and other Wireless Router or Access Point. If your Wireless Router or Access Point also supports WPS function, users can activate WPS auto-encryption to speed up the procedures.

WPS supports 2 models: PIN (Personal Information Number) and PBC (Push Button Configuration). These models are approved by the Wi-Fi Alliance.

PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

*The following figure is the display of the front of CQR-981.



When users select a specific model on wireless base station, the clients can connect to the base by selecting the same model.

The connection procedures of PIN and PBC are almost the same. The small difference between those two is:

Users input the PIN of wireless card in the base station first; it will limit the range of the clients. It is faster to establish a connection on PIN model.

On PBC model, users push the WPS button to activate the function, and then the wireless client must push the WPS button in 2 mins to enter the network. The client will search to see if there is any wireless base station which supports WPS is activating. If the client finds a matching base, the connection will be established. The speed of establishing a connection is slower than the PIN model because of this extra step.

On the other hand, users need to input the information of the wireless card into the register interface. It might lead to the failure of connection, if users make mistakes on inputting. On PBC model, users only need to click the WPS button on both sides to make a connection. It is easier to operate.

This page supports **Start PBC** and **Start PIN**; please follow the instructions to operate.

*** Start PBC:**

(1) Please click **Start PBC** to connect to the other Wireless Router.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

Self-PIN Number: 51039615

PIN Configuration:

Push Button Configuration:

(2) Please click **OK** to start WPS process.

Start PBC successfully!

You have to run Wi-Fi Protected Setup in AP within 2 minutes.

(3) Open the configuration page of the Wireless Router, like CWR-935 which supports WPS. Click the **WPS** page, and then click **Start PBC** to make a WPS connection.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status:

☒ Configured ☐ Un-Configured

Self-PIN Number:

73220398

Push Button Configuration:

Start PBC

Apply Change

Reset

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

Start PIN

(4) Click **OK** to start WPS process.

Start PBC Successfully You have to run Wi-Fi Protected Setup in Client within 2 minutes.

OK

(5) When WPS process finish, please check the Wireless Configuration of CQR-981, you can find CQR-981 already connect to CWR-935 via WPS.

WirelessConfiguration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	CWR-935
Channel Number	11
Encryption	Disabled
MAC	00:d0:41:b9:e2:83
State	Connected

*** Start PIN:**

- (1) Please open the WPS configuration page of the CQR-981 to get a PIN number, and write it down.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

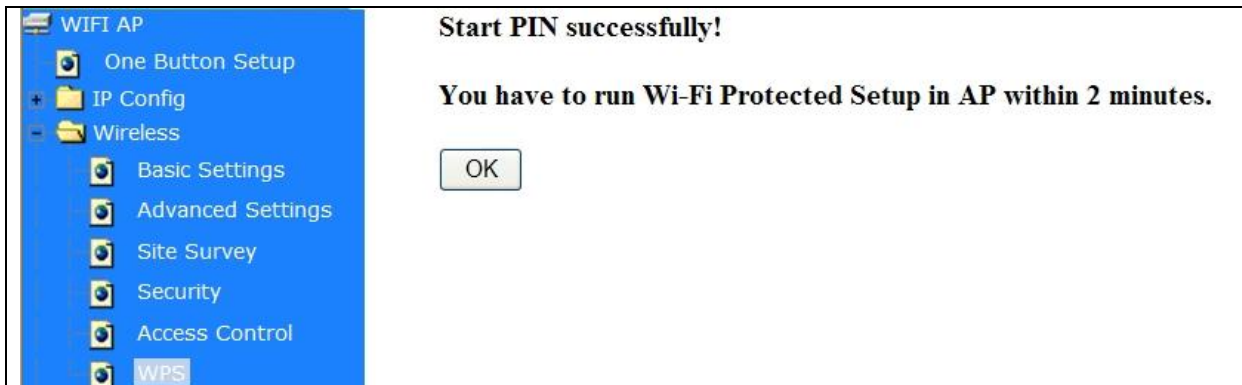
☐ Disable WPS

Self-PIN Number: 25932195

PIN Configuration:

Push Button Configuration:

- (2) Please click **OK** to start WPS process..



WIFI AP

- One Button Setup
- IP Config
- Wireless
 - Basic Settings
 - Advanced Settings
 - Site Survey
 - Security
 - Access Control
 - WPS**

Start PIN successfully!

You have to run Wi-Fi Protected Setup in AP within 2 minutes.

- (3) Open the configuration page of the Wireless Router, like CWR-935 which supports WPS. Click the **WPS** page, fill the WPS PIN code.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status: ☒ Configured ☐ Un-Configured

Self-PIN Number: 73220398

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

25932195

(4) Click **OK** to starts process.

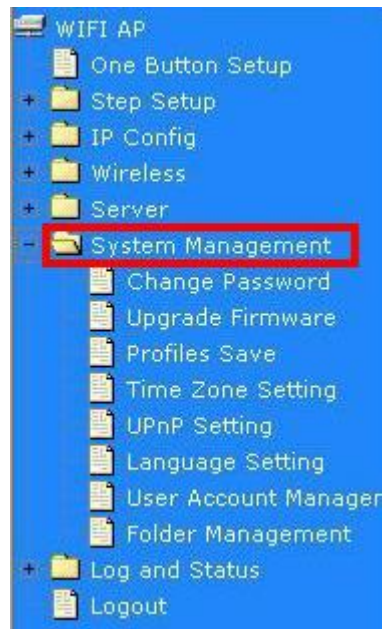
Applied client's PIN successfully! You have to run Wi-Fi Protected Setup in Client within 2 minutes.

(5) When WPS process finish, please check the Wireless Configuration of CQR-981, you can find CQR-981 already connect to CWR-935 via WPS.

WirelessConfiguration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	CWR-935
Channel Number	11
Encryption	Disabled
MAC	00:d0:41:b9:e2:83
State	Connected

6.3 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.



6.3.1 Change Password

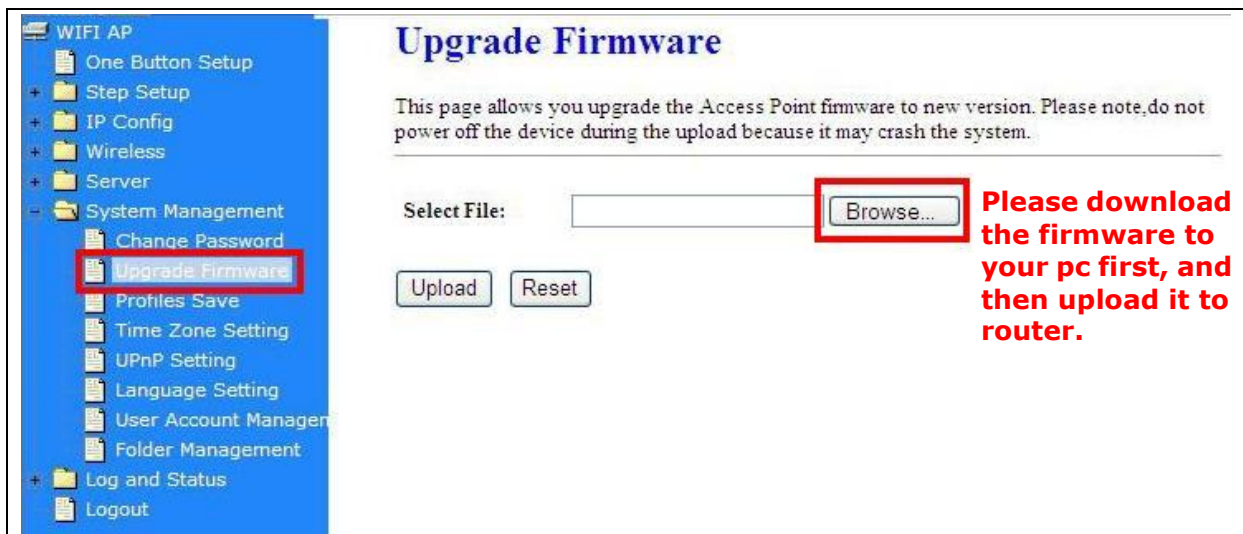
Users can set or change their password in this section.

A screenshot of the 'Password configuration' page. On the left, the same blue sidebar is shown, with 'Change Password' highlighted by a red box. The main content area has a title 'Password configuration' and a description: 'This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.' Below this, there are three input fields: 'User Name:' with the value 'admin', 'New Password:', and 'Confirmed Password:'. The 'New Password' and 'Confirmed Password' fields are grouped by a red box. To the right of these fields, red text reads: 'Please input the new password and confirm it.' At the bottom, there are two buttons: 'Apply Change' and 'Reset'.

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6.3.2 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website (<http://www.cnet.com.tw>) to see if there is any later version of firmware. Download the firmware to your computer, click **Browser** and point to the new firmware file. Click **Upload** to upgrade the firmware. You can't make any move unless the machine reboot completely.

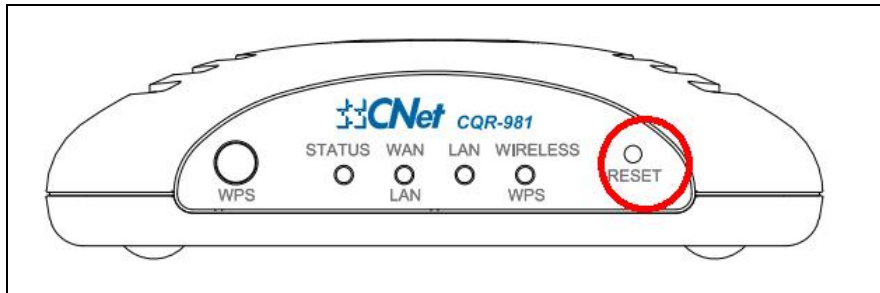


Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Caution: The firmware upgrade will not remove your previous settings.

* Reset button:

On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



6.3.1 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File: **Save to computer**

Load Settings from File: **Upload the file from PC to router**

Reset Settings to Default: **Reset to default.**

a. Save Configuration

(1) Click **Save**

Save/Reload Settings

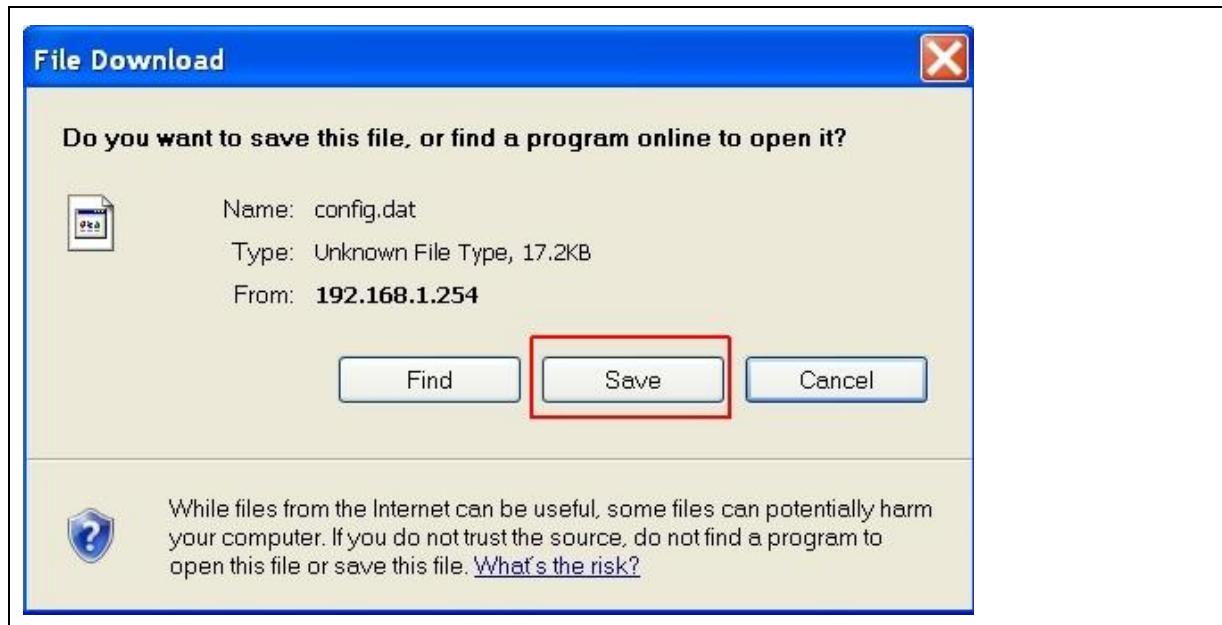
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

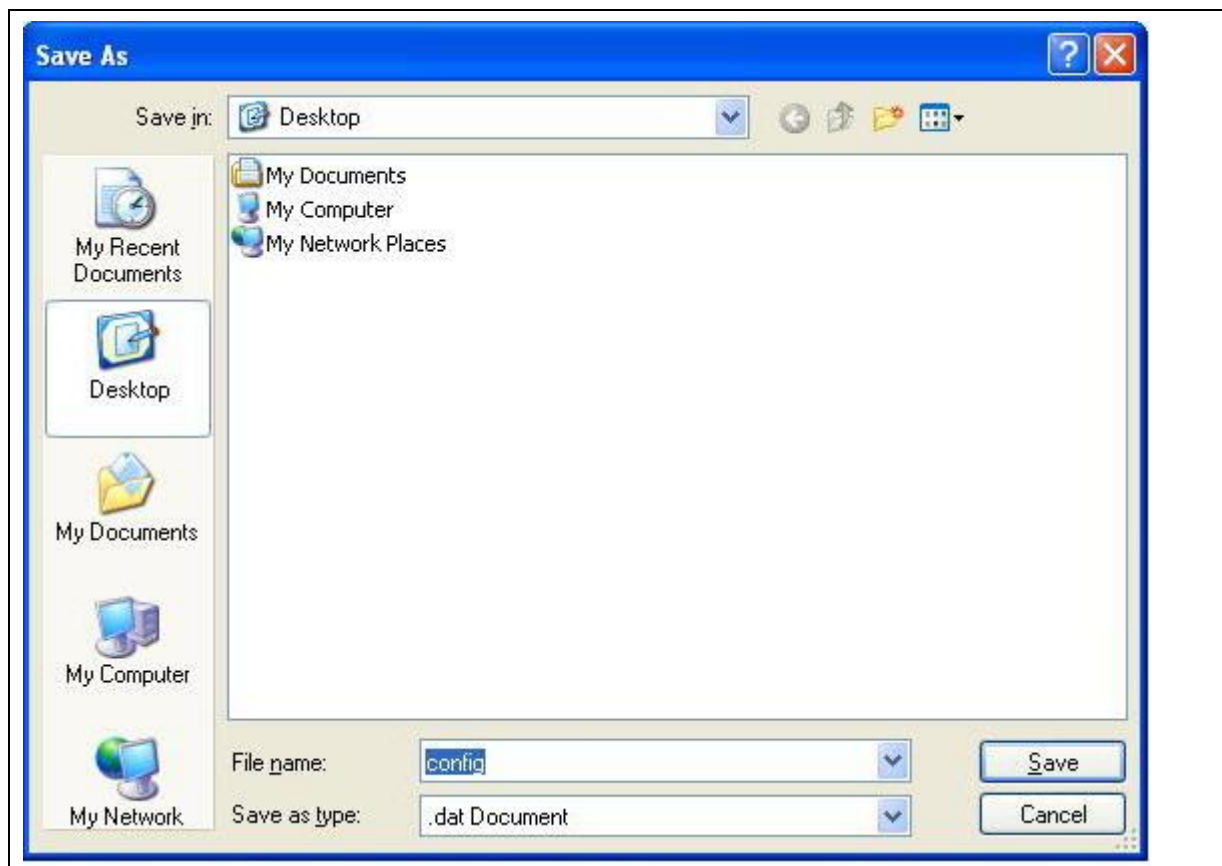
Load Settings from File:

Reset Settings to Default:

(2) Please click "Save" to save the configuration to your computer.



(3) Select the location which you want to save file, then click **Save**.



b. Load configuration file

(1) Click **Browser**

Save/Reload Settings

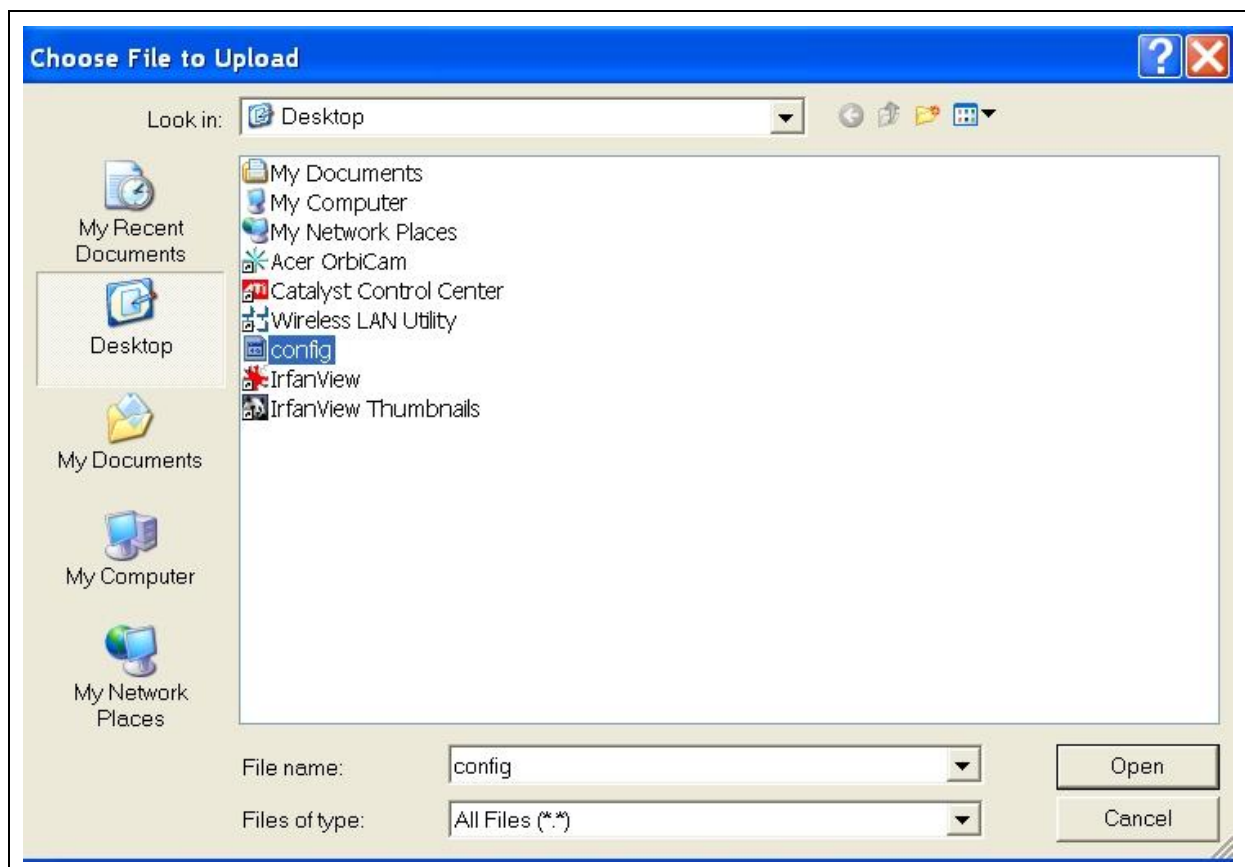
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(2) Select configuration file then click **Open**



(3) Click **Upload** to upload configuration file to CQR-981.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(4) After 90 seconds, CQR-981 will reboot automatically.

(C) Reload factory default setting

1. Please click **Reset**

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.


Save Settings to File:

Load Settings from File:

Reset Settings to Default:

(2) Please click **OK** to start reload factory default setting to CQR-981.

Message from webpage

 Do you really want to reset the current settings to default?

(3) After 90 seconds, CQR-981 will reboot automatically.


6.3.2 Time Zone Setting

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.

Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :  Please select the time zone

☒ Enable NTP client update

☐ Automatically Adjust Daylight Saving

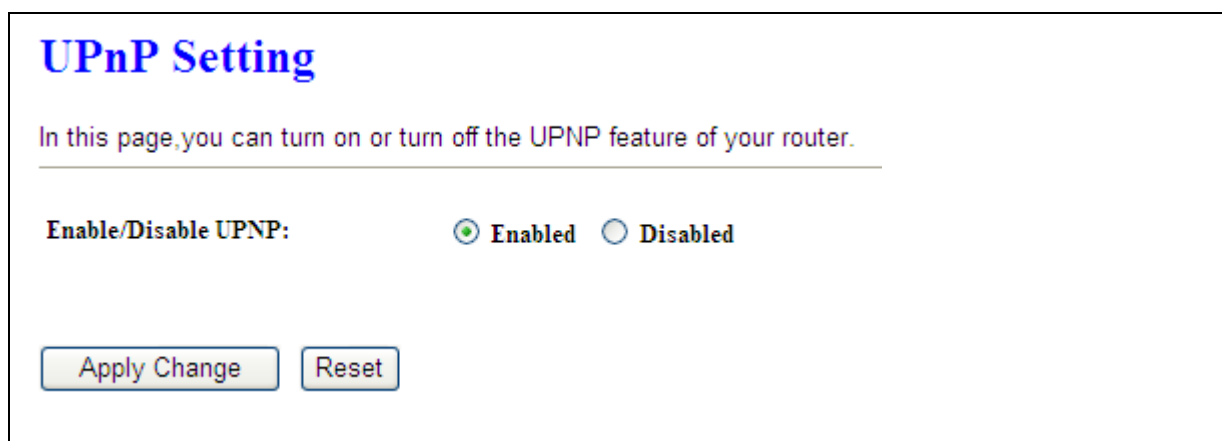
NTP server : ☒ 

☐ (Manual IP Setting)

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable Automatically Adjust Daylight Saving or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data. Or you may click on Refresh to update the system time on the screen.

6.3.3 UPnP Setting

Universal Plug and Play (UPnP) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. CQR-981 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My Network Places**. Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.



*Enable/Disable UPnP

Select to enable or disable this function.

6.4 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



6.4.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP ...information.

System	
Uptime	0day:17h:37m:55s
Firmware Version	Ver1.0.2
WirelessConfiguration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	CQR-981

6.4.2 Event Log

You may enable the event log feature here.

☐ Enable Log → Please select to enable log function.

☐ system all ☐ wireless ☐ DoS

☐ Enable Remote Log Log Server IP Address:

Item	Description
Enable Log	You may choose to enable Event Log or not.
System all, Wireless, & DoS	Please select the event you want to record.

Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply Changes & Refresh & Clear	Click on Apply Changes to save the setting data. Click on Refresh to renew the system time, or on Clear to clear all the record.

* The following figure is an example when users click **Apply Changes** to record the event log.

☒ **Enable Log**
☒ **system all** ☐ **wireless** ☐ **DoS**
☐ **Enable Remote Log** Log Server IP Address:

```

ComntTrack
Oday 00:00:17 PPTP netfilter connection tracking: registered
Oday 00:00:17 PPTP netfilter NAT helper: registered
Oday 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
Oday 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
Oday 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
Oday 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
Oday 00:00:17 Freeing unused kernel memory: 64k freed
Oday 00:00:17 mount /proc file system ok!
Oday 00:00:17 mount /var file system ok!
Oday 00:00:17 device eth0 entered promiscuous mode
Oday 00:00:17 device wlan0 entered promiscuous mode
Oday 00:00:17 TPT: unreasonable target TSSI 0
Oday 00:00:17 br0: port 2(wlan0) entering listening state
Oday 00:00:17 br0: port 1(eth0) entering listening state
Oday 00:00:17 br0: port 2(wlan0) entering listening state
  
```


6.5 Logout

This function logs out the user.

WIFI AP

- One Button Setup
- IP Config
- Wireless
- System Management
- Log and Status
- Logout

Logout

This page is used to logout.

Do you want to logout ?

Click on Apply Change to logout.

Chapter 7 DDNS Account Setup

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

【Step 1】

Please visit the website <http://www.dyndns.com/>, and click on **Sign Up Now**.



The screenshot shows the DynDNS website homepage. At the top left is the DynDNS logo. To the right of the logo are input fields for 'User:' and 'Pass:' with a login button. Below the login fields are links for 'Lost Password?' and 'Sign Up Now'. A yellow navigation bar contains links for 'About', 'Services', 'Account', 'Support', and 'News'. The main content area features a large black banner with a globe graphic and the text 'Keep Connected with DynDNS'. To the right of the banner is a list of services: DNS, E-mail, Network Monitoring, and Redirection. Below the banner, there are three main sections: 'A Leader in DNS Services' (describing DynDNS services), 'Domain Registration' (with a text input field for 'www. yourdomain.com' and a 'Get Started' button), and 'News' (with a link to 'Select Patton Electronics Devices Now DynDNS Certified'). On the right side of the page, there are two sidebar sections: 'Custom DNS' (describing primary DNS services) and 'Resources' (listing links for Business Solutions, Home Solutions, What is DNS?, Why DynDNS?, Careers with DynDNS, and Developer's Connection). At the bottom right is a 'Premier Support' section.

【Step 2】

Please fulfill the requested information at the column, and click on **Create Account** when finished. (The information shown on the screen is for your reference only)

Acceptable Use Policy

1. ACKNOWLEDGMENT AND ACCEPTANCE OF TERMS OF SERVICE

All services provided by Dynamic Network Services, Inc. ("DynDNS") are provided to you (the "Member") under the Terms and Conditions set forth in this Acceptable Use Policy ("AUP") and any other operating rules and policies set forth by DynDNS. The AUP comprises the entire agreement between the Member and DynDNS and supersedes all prior agreements between the parties regarding the subject

I have read and agree to the Acceptable Use Policy above: ☒

Username

Username

Your username will be used to login to your account and make changes.

E-mail Address

E-mail Address Confirm E-mail Address:

The e-mail address you enter must be valid. Instructions to activate your account will be sent to the e-mail address provided. You must keep this address current. Any accounts with invalid e-mail addresses are subject to removal without warning. We do not sell our list to anyone. Read more about our [privacy policy](#).

Password

Password Confirm Password

The password you enter will be used to access your account. It must be more than 5 characters and cannot be your username.

Optional Information


How did you hear about us: Details:

Providing this information will help us to better understand our customers, and tailor future offerings more accurately to your needs. Thanks for your help!

Create Account

【Step 3】

When the below window appears, you already finish the registration. Please check your E-mail box, and you will receive an e-mail from the DynDNS.


DynDNS

User:
Pass:

[Lost Password?](#) - [Sign Up Now](#)

My Account	About	Services	Account	Support	News
Create Account	Account Created				
Login	<p>Your account, navi, has been created. Directions for activating your account have been sent to navi@etopnetwork.com.tw. To complete registration, please follow the directions that you will receive. You must complete these steps within 48 hours to complete your registration.</p> <p>You should receive the confirmation e-mail within a few minutes. Please make certain that your spam filtering allows messages from support@dyndns.com to be delivered. If you have not received this e-mail within an hour or so, request a password reset.</p> <p>Following the instructions in the password reset e-mail will also confirm your new account. If you don't receive the password reset e-mail either, you should check with your e-mail provider to determine why you are not receiving these messages.</p>				
Lost Password?					

【Step 4】

Please open the email sent from DynDNS.

Click on the link to confirm your account.

Inbox

From	Subject
DynDNS Support	Your DynDNS Account Information

Your DynDNS Account Information

DynDNS Support [support@dyndns.com]

TO: navi@etopnetwork.com.tw

Your DynDNS user account 'navi' has been created. You must visit the confirmation address below within 48 hours of the time this e-mail was sent to complete the account creation process.

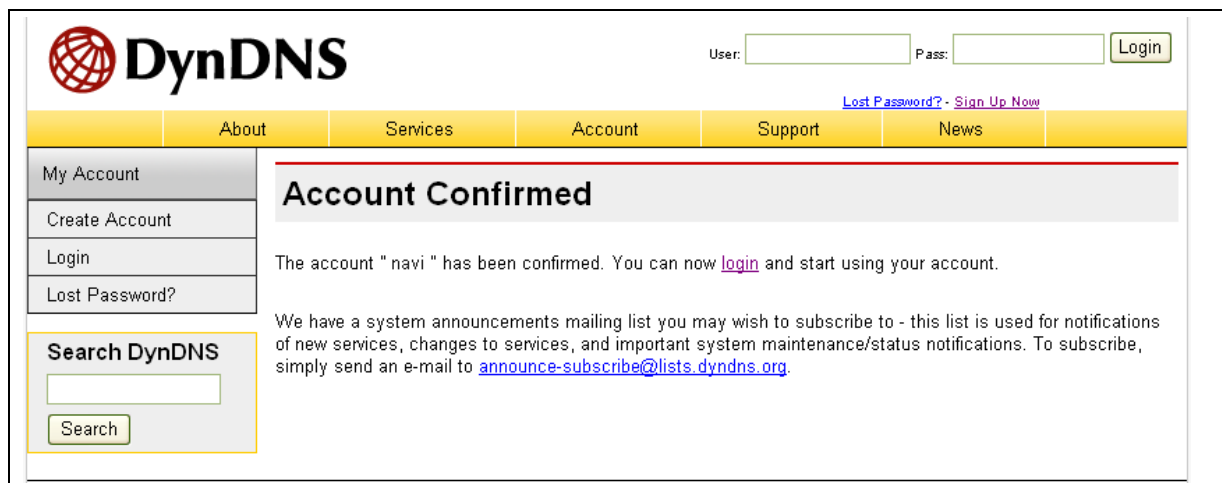
Our basic service offerings are free, but they are supported by our premium services. See <http://www.dyndns.com/services/> for a full listing of all of our available services.

To confirm your account, please go to the address below:

<https://www.dyndns.com/account/confirm/wRf7xNbusv8rsSUqt6-USw>

【Step 5】

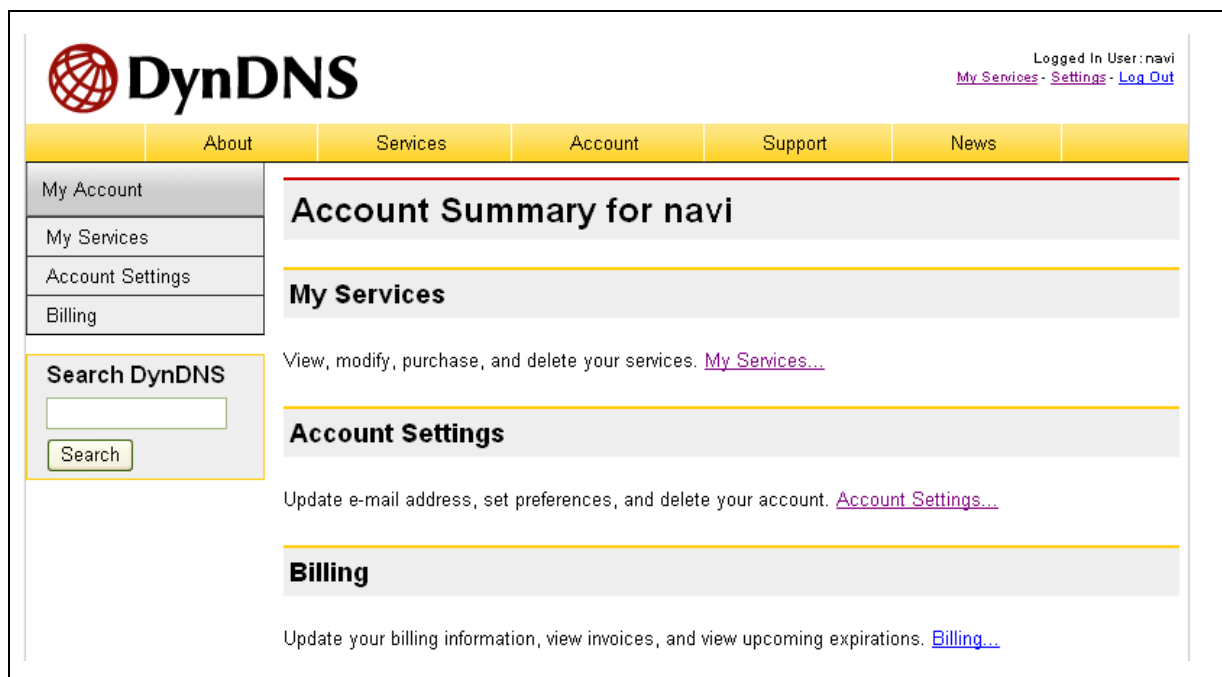
Please click on **login**.



The screenshot shows the DynDNS website interface. At the top left is the DynDNS logo. To the right of the logo are input fields for 'User:' and 'Pass:', followed by a 'Login' button. Below the login fields is a navigation bar with links: 'About', 'Services', 'Account', 'Support', and 'News'. On the left side, there is a 'My Account' menu with options: 'Create Account', 'Login', and 'Lost Password?'. Below this menu is a 'Search DynDNS' section with a search input field and a 'Search' button. The main content area displays a message titled 'Account Confirmed'. The text reads: 'The account "navi" has been confirmed. You can now [login](#) and start using your account.' Below this, it mentions a mailing list for system announcements and provides an email address: announce-subscribe@lists.dyndns.org.

【Step 6】


Please click on **My Services** under the Account Summary for the linkage.



The screenshot shows the DynDNS website interface after logging in. The top right corner indicates 'Logged In User: navi' with links for 'My Services', 'Settings', and 'Log Out'. The navigation bar remains the same. The 'My Account' menu now includes 'My Services' along with 'Account Settings' and 'Billing'. The main content area displays the 'Account Summary for navi' page. It features three main sections: 'My Services' with a link to 'My Services...', 'Account Settings' with a link to 'Account Settings...', and 'Billing' with a link to 'Billing...'. Each section has a brief description of what can be managed there.

【Step 7】

Please click on **Add Host Services**.


DynDNS

Logged In User: navi
[My Services](#) - [Settings](#) - [Log Out](#)

[About](#)
[Services](#)
[Account](#)
[Support](#)
[News](#)

My Account
 My Services
 Account Upgrades
 MailHop Outbound
 Recursive DNS
 SLA
 Premier Support
 My Zones
 Add Zone Services
 My Hosts
 Add Host Services
 Account Settings
 Billing

Search DynDNS

Account Level Services

Credited Account (?)	No	Technical Support
Account Upgrades (?)	No	View - Add
MailHop Outbound (?)	None	View - Add
Recursive DNS (?)	None	View - Add
DNS Service Level Agreement (?)	None	View - Add
Premier Support Option (?)	None Available	Add Premier Support Cases

Zone Level Services

[Add Zone Services](#)

No zone level service items registered.

Host Level Services

[Add Host Services](#)

Host	DNS Service	WebHop	Network Monitoring
navi.ath.cx	Dynamic DNS		

【Step 8】

Please click on **Add Dynamic DNS Host**.

[About](#)
[Services](#)
[Account](#)
[Support](#)
[News](#)

My Account
 My Services
 Account Upgrades
 MailHop Outbound
 Recursive DNS
 SLA
 Premier Support
 My Zones
 Add Zone Services

Add Host Services

Dynamic DNS (?)	Add Dynamic DNS Host
Static DNS (?)	Add Static DNS Host
WebHop (?)	Add WebHop
MyWebHop (?)	Add MyWebHop
Network Monitoring (?)	Add Network Monitoring

【Step 9】

1. Please input the account you applied.
2. Please select the hostname preferred at the drop-down menu.
3. Please click on **Add Host** to add the name.


New Dynamic DNSSM Host

Hostname:	1	navi	ath.cx	2
IP Address:		59.120.102.70		
Enable Wildcard:		<input type="checkbox"/>		
Mail Exchanger (optional):			<input type="checkbox"/> Backup MX?	

3
Add Host
Reset Form

【Step 10】

When the below window appears, it means your hostname is created.


DynDNS

[About](#)
[Services](#)
[Account](#)
[Support](#)
[News](#)

My Account
My Services
Account Upgrades
MailHop Outbound
Recursive DNS
SLA
Premier Support
My Zones
Add Zone Services
My Hosts
Add Host Services

Hostname Created

The hostname you have requested has been created. The information now in the database and DNS system is

Hostname:	navi.ath.cx
IP Address:	59.120.102.70
Wildcard:	N
Mail Exchanger:	None
Backup MX:	N

Chapter 8 Q & A

8.1 Installation

1. Q: Where is the XDSL Router installed on the network?

A: In a typical environment, the Router is installed between the XDSL line and the LAN. Plug the XDSL Router into the XDSL line on the wall and Ethernet port on the Hub (switch or computer).

2. Q: Why does the throughput seem slow?

A: To achieve maximum throughput, verify that your cable doesn't exceed 100 meter. If you have to do so, we advise you to purchase a bridge to place it in the middle of the route in order to keep the quality of transmitting signal. Out of this condition you would better test something else.

- Verify network traffic does not exceed 37% of bandwidth.
- Check to see that the network does not exceed 10 broadcast messages per second.
- Verify network topology and configuration.

8.2 LED

1. Why doesn't 11n Broadband Router power up?

A: Check if the output voltage is suitable, or check if the power supply is out of order.

2. The Internet browser still cannot find or connect to 11n Broadband Router after verifying the IP address and LAN cable, the changes cannot be made, or password is lost.

A: In case 11n Broadband Router is inaccessible, you can try to restore its factory default settings. Please press the "Reset" button and keep it pressed for over 7 seconds and the light of STATUS will vanish. The LEDs will flash again when reset is successful.

3. Why does 11n Broadband Router shut down unexpectedly?

A: Re-plug your power adapter. Then, check the STATUS indicator; if it is off, the internal flash memory is damaged. For more help, please contact with your provider.

8.3 IP Address

1. Q: What is the default IP address of the router for LAN port?

A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0

2. Q: I don't know my WAN IP.

A: There are two ways to know.

Way 1: Check with your Internet Service Provider.

Way 2: Check the setting screen of 11n Broadband Router. Click on **Status & Log** item to select **Network Configuration** on the Main Menu. WAN IP is shown on the WAN interface.

3. How can I check whether I have static WAN IP Address?

A: Consult your ISP to confirm the information, or check Network Configuration in 11n Broadband Router's Main Menu.

4. Will the Router allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Router?

A: Yes, the Router mode allows for customization of your public IPs and Domain.

8.4 OS Setting

1. Why can't my computer work online after connecting to 11n Broadband Router?

A: It's possible that your Internet protocol (TCP/IP) was set to use the following IP address. Please do as the following steps. (Windows 2000 & XP) **Start > Settings > Network and Dial-up Connections > double click on Internet Protocol(TCP/IP) > select obtain IP address automatically > Click on OK button.** Then, open Internet browser for testing. If you still can't go online, please test something else below.

- Verify network configuration by ensuring that there are no duplicate IP addresses.
- Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.
- 1. Check that the cables and connectors or use another LAN cable.

2. Q: Web page hangs, corrupt downloads, or nothing but junk characters is being

displayed on the screen. What do I need to do?

A: Force your NIC to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your NIC as a temporary measure. (Please look at the Network Control Panel, in your Ethernet Adapter's Advanced Properties tab.)

3. Q: Why can't I connect to the Web Configuration?

A: you can remove the proxy server settings in your web browser.

8.5 11n Broadband Router Setup

1. Q: Why does 11n Broadband Router's setup page shut down unexpectedly?

A: If one of the pages appears incompletely in 11n Broadband Router's setup pages, please click on Logout item on the Main Menu before shutting it down. Don't keep it working. Then, close Internet browser and open it again for going back to the previous page.

2. Q: Why can't my USB devices and LAN ports work properly after setting the DHCP?

A: There are two rules over here.

Rule1: After connecting USB devices, please reboot your Router.

Rule2: Before finishing the DHCP setup, please don't connect any computer to LAN ports, because the conflict of having the same IP may occur and cause some computers a lot of trouble.

※Notice: Make sure that you always click on the Apply button after configuring each setting. And in order to let other LAN ports work properly, please reboot your PC.

3. Q: I don't know how to configure DHCP.

A: DHCP is commonly used in the large local network. It allows you to manage and distribute IP addresses from 2 to 254 throughout your local network via 11n Broadband Router. Without DHCP, you would have to configure each computer separately. It's very troublesome. Please Open **Internet browser** > Input **192.168.1.1 in the website blank field** > Select **DHCP Server under the IP Config Menu**. For more information, please refer to 3.3.2 (Router Mode) or 4.3.1 (AP Mode).

4. Q: How do I upgrade the firmware of 11n Broadband Router?

A: Periodically, a new Flash Code is available for 11n Broadband Router on your product supplier's website. Ideally, you should update 11n Broadband Router's Flash Code using **Upgrade Firmware** on the **System Management** menu of 11n Broadband Router Settings.

5. Q: My 11N Broadband Router cannot connect to the ISP?

A: There are three possible solutions.

1. Check the Cable/XDSL modem is power on.
2. Check the Cable/XDSL link light is on to verify a good physical connection.
3. Check the WAN port LED to verify if the Cable/XDSL modem is connected to the router:

If your ISP Login method is following, please make sure the username and password are correct or not.

If your ISP is using dynamic IP addressing (DHCP) then the DHCP protocol does not have the authentication feature. Some Cable service providers often use the following to determine user's identification.

6. Q: Why is that I can ping to outside hosts, but cannot access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router assign the DNS settings to the DHCP-client-enabled PC.

7. Q: 11n Broadband Router couldn't save the setting after click on Apply button?

A: 11n Broadband Router will start to run after the setting finished applying, but the setting isn't written into memory. Here we suggest if you want to make sure the setting would be written into memory, please reboot the device via **Reboot** under **System Management** directory.

8.6 Wireless LAN

1. Q: Why couldn't my wireless notebook work on-line after checking?

A: Generally, Wireless networks can sometimes be very complicated to set up, particularly if you're dealing with encryption and products from different vendors. Any number of variables can keep your workstations from talking to each other. Let's go over some of more common ones.

For starters, verify that your router and your workstation are using the same SSID descriptions. SSID acts as a password when a mobile device tries to connect to the wireless network. The SSID also differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A workstation will not be permitted to connect to the network unless it can provide this unique identifier. This is similar to the function of your network's Workgroup or Domain name.

When you're experiencing conductivity problems, it is always best to keep things simple. So next you are going to do is that, please disable any WEP encryption you might have configured.

Successful implementation of encryption also includes the use of a shared key. A HEX key is the most common, but other formats are also used. This key identifies the workstation to the router as a trusted member of this network. Different manufacturers can implement this key technology in ways that might prevent them from working correctly with another vendor's products. So pay attention to detail is going to be the key to a successful installation.

Next make sure the router and the NIC are configured to use the same communications channel. There are normally 11 of them, and the default channel can also vary from vendor to vendor. You might also want to confirm that the router has DHCP services enabled and an address pool configured. If not, the NIC won't be able to pick up an IP address. I have run across a few access points that offer DHCP services but do not assign all of the needed IP information to the NIC. As a result, I was able to connect to the network, but could not browse the web. The point is, don't assume anything. Verify for yourself that all of the required settings are being received by the workstation.

Finally, you might want to keep the system you're trying to configure in the same room as the router, at least during the initial configuration, in order to minimize potential interference from concrete walls or steel beams.

2. Q: My PC can't locate the Wireless Access Point.

A: Check the following:

- Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode.)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Router's Wireless screen is set to Allow LAN access to selected Wireless Stations only, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

3. Q: Wireless connection speed is very slow.

A: The wireless system will connect at highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with following:

- Access Point location: Try adjusting the location and orientation of the Access Point.
- Wireless Channel: If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference: Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding: Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

4. Q: Some applications do not run properly when using the Wireless Router.

A: The Wireless Router processes the data passing through it, so it is not transparent. Use the Special Application feature to allow the use of Internet applications which do not function correctly. If this does solve the problem, you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

5. Q: I can't connect to the Wireless Router to configure it.

A: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Wireless Router are on the same network segment.
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, make sure that it is using an IP Address within the range 192.168.1.129 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using Control Panel ~ Network to check the Properties for the TCP/IP protocol.

6. Q: The WinXP wireless interface couldn't communicate the WEP with 11n Broadband Router's wireless interface.

A: The default WEP of WinXP is **Authentication Open System - WEP**, but the WEP of 11n Broadband Router is only for **Shared Key - WEP**, it caused both sides couldn't communicate. Please select the WEP of WinXP from Authentication Open System to **Pre-shared Key - WEP**, and then the WEP wireless interface between WinXP and 11n Broadband Router would be communicated.

8.7 Support

1. Q: What is the maximum number of IP addresses that the XDSL Router will support?

A: The Router will support to 253 IP addresses with NAT mode.

5. Q: Is the Router cross-platform compatible?

A: Any platform that supports Ethernet and TCP/IP is compatible with the Router.

8.8 Others

1. Q: Why can't I receive corrupted FTP downloads?

A: If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

2. Q: Why does the router dial out for PPPoE mode very often?

A: Normally some of game, music or anti-virus program will send out packets that trigger the router to dial out, you can close these programs. Or you can set the idle time to 0, then control to dial out manually.

3. Q: What can I do if there is already a DHCP server in LAN?

A: If there are two DHCP servers existing on the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually.